CHAPTER FOUR
TERRORISM: MANAGING TODAY'S THREAT

Summary & Findings

As part of the Commission's charter to assess whether the Intelligence Community is properly postured to support the U.S. government's efforts to respond to the threats of the 21st century, we reviewed the progress the Intelligence Community has made in strengthening its counterterrorism capabilities since the September 11 attacks. We found that, although the Community has made significant strides in configuring itself to better protect the homeland and take the fight to terrorists abroad, much remains to be done to ensure the efficient use of limited resources among agencies responsible for counterterrorism intelligence. The U.S. government has not yet successfully defined the roles, missions, authorities, and the means of sharing information among our national and homeland security organs. Specifically, we found that:

- Information flow between the federal, state, local, and tribal levels—both up and down—is not yet well coordinated;
- Ambiguities in the respective roles and authorities of the National Counterterrorism Center and the Intelligence Community-wide Counterterrorist Center have not been resolved;
- Persistent conflicts over the roles, missions, and authorities of counterterrorism organizations may limit the Community's ability to warn of potential threats;
- Confusion and conflict regarding the roles, missions, and authorities of counterterrorism organizations have led to redundant efforts across the Community and inefficient use of limited resources; and
- The failure to manage counterterrorism resources from a Community perspective has limited the Intelligence Community's ability to understand and warn against terrorist use of weapons of mass destruction.

INTRODUCTION

Providing intelligence that facilitates the global war on terrorism and warns against terrorist use of weapons of mass destruction is currently the Intelligence Community's most vital mission. There is every reason to believe that this will remain the top priority for a generation or more. As a result, it is impossible to reach broad conclusions regarding the Intelligence Community's overall performance, and develop meaningful suggestions for improvement and reform, without an understanding of Intelligence Community capabilities with regard to countering the terrorist threat—both now and in the future.

We did not set out to study "terrorism" writ large; such an ambitious endeavor is beyond the scope and time allotted to this Commission. Rather, we chose to focus narrowly on examining several well-documented weaknesses inherent in the Intelligence Community's counterterrorism capabilities prior to the September 11 attacks, and on measures the Intelligence Community has subsequently taken to remedy those deficiencies. Our work thus focused on four primary areas:

1. The status of *information sharing* among federal agencies with foreign and domestic intelligence and law enforcement responsibilities, as well as between federal agencies and state, local, and tribal law enforcement;

2. The effectiveness of the *threat-warning* mechanism by which policymakers are kept informed of potential terror threats;

3. The ability to synthesize relevant *all-source terrorism analysis* in a timely manner; and

4. The Intelligence Community's ability to provide the intelligence necessary to interdict a planned *terrorist attack using a weapon of mass destruction.*

We conclude that although the Intelligence Community has made significant strides in each of these areas, much remains to be done. We found substantial evidence that information flows between the federal level and the state, local, and tribal levels—both upward and downward—are not yet well coordinated.

The roles and responsibilities among Intelligence Community agencies charged with primary responsibility for terrorism intelligence—both tactical and strategic—are not clearly defined. Sustained bureaucratic infighting and poor coordination prevent the Community from optimizing its resources to fight terrorism and alert policymakers to terrorist threats. Moreover, Community efforts to integrate technical and regional intelligence expertise with counterterrorism analysis do not provide sufficient focus on the threat posed by weapons of mass destruction in the hands of terrorists.

Resolving complex bureaucratic issues that transcend agency and subject-matter boundaries is usually difficult. However, three and a half years removed from the September 11 attacks, the persistence of agency coordination problems and unclear definitions of responsibility suggest to us a lack of Community leadership. The intelligence entities responsible for counterterrorism, especially terrorism analysis and threat warning, must be properly aligned, supported, and integrated for the task at hand.

SYSTEMIC FLAWS AS OF THE "SUMMER OF THREAT"

It is well-established that the Intelligence Community's structure and practices prior to the September 11 attacks were simply not up to the task of waging a global war on terror and protecting the homeland. The systemic Intelligence Community deficiencies during the "Summer of Threat" leading up to the attacks were summed up by the 9/11 Commission in two short sentences: "Information was not shared… Analysis was not pooled."[1] For present purposes, we highlight three of the specific failings identified by the 9/11 Commission in its examination of the Intelligence Community before September 11.

First, prior to September 11, there was a failure to share terrorism-related information rapidly and efficiently within agencies; among entities within the Intelligence Community tasked with producing intelligence to support counterterrorism efforts, and with state, local, and tribal law enforcement. For example, the FBI lacked basic computer capabilities, and did not share information even within its own organization. The CIA and the FBI were unwilling or unable to exchange information quickly and effectively with each other. And the Immigration and Naturalization Service and FBI did not learn from

the CIA which identified terrorists were entering the United States and where they might be.[2]

Second, the Intelligence Community's analysts were ill-equipped to "connect the available dots" that might have led to advance warning of the September 11 attacks.[3] The "dispersal of effort on too many priorities" and the "declining attention to the craft of strategic analysis" were among the shortcomings identified by the 9/11 Commission's staff.[4] The CIA published many useful analytical reports on terrorism before the attack, but the Intelligence Community failed to produce a comprehensive, cross-cutting assessment of the threat. Analysts had difficulty carving out time to work on longer-term analyses that could have unified disparate elements of intelligence and pointed to the existence of a growing threat or particular vulnerability.[5]

Third, there was a lack of coordinated effort among the major federal agencies tasked with counterterrorism responsibilities, and confusion as to the roles and responsibilities of those agencies. Because the CIA and FBI lacked an optimized, cooperative analytical and operational effort, they were not well configured to detect and counter a threat, like that posed by the September 11 plotters, which "fell into the void between foreign and domestic threats." [6]

NOTABLE IMPROVEMENTS SINCE THE SEPTEMBER 11 ATTACKS

We found evidence that this grim picture has improved in many respects since September 11. In the information sharing arena, for example, consolidation of terrorist "watchlists" and expanded use of those lists for screening purposes have increased the likelihood of detecting known or suspected terrorists and obtaining additional information about them.[7] Moreover, counterterrorism information sharing has increased in quantitative terms—that is, terrorism intelligence products are disseminated more broadly, and are produced by more agencies, than before September 11.[8]

Similarly, the Intelligence Community has remedied many of the analysis-related problems it faced leading up to the September 11 attacks. In particular, the Community increased its analytic efforts on terrorism-related issues, including analytic support to operations, and at the President's direction established the Terrorist Threat Integration Center (TTIC, now the National

Counterterrorism Center, or NCTC) as the Community's center for analysis on these topics.[9] Many analysts arrive with substantial experience gained from working on terrorism accounts at the DCI's Counterterrorist Center (CTC),[10] an organization originally based at the CIA and staffed primarily by CIA officers that also includes representatives from throughout the Community. Analysts are increasingly being assigned to the NCTC for two-year rotations instead of short-term, stop-gap stints, enabling it to develop some badly-needed depth of expertise among its analytic corps.[11] Perhaps most significantly in light of the criticisms leveled by the 9/11 Commission, the NCTC is producing analytic products that integrate the comments and concerns of analysts across the Community.[12]

Moreover, the President's Terrorist Threat Report, a daily analytic publication produced by the NCTC, is truly a Community effort—with five agencies regularly contributing and a production schedule established by regular interagency meetings.[13] Prior to the September 11 attacks, it was far from clear that the intelligence resources of all the relevant agencies in the Intelligence Community were being tapped to create a complete picture of terror threats for senior policymakers. In contrast, the NCTC now hosts "ecumenical" meetings five days a week, in which managers representing CIA, FBI, DIA, NSA, and the Departments of State and Homeland Security[14] share and discuss intelligence regarding key terror threats.[15] The NCTC also meets five times weekly with senior representatives of CIA, FBI, DIA, and Homeland Security at a formal planning production board to divide responsibility for drafting analytical products (mainly those which will appear in the President's threat report) and to share information.[16] This process represents a level of formal and informal interaction on the terrorist threat among the primary intelligence agencies that simply did not exist prior to September 11, and that seems to clearly represent an improvement in the identification of threats and the mechanism through which threat warning intelligence is provided to senior policymakers.[17]

In our view the overall quality of finished analytic pieces on terrorism has also improved. Analysts in the Community now have access to substantially more information as the result of the Intelligence Community's heightened prioritization of the terrorism issue, the availability of intelligence from new collectors (particularly FBI and Homeland Security), and expanded access to information about human intelligence sources.[18]

Perhaps most importantly, from an operational perspective it is clear that many of CTC's efforts to disrupt terrorist networks and plots—partially enabled by its in-house analytic cadre—have been extraordinary successes. Put simply, CTC has brought the fight to the terrorists.

Finally, we have found that September 11 and the subsequent anthrax attacks not only triggered an aggressive counterterrorism response throughout the U.S. government, but also prompted the Community to reconsider its approach to the possible acquisition and use of weapons of mass destruction by terrorists, which we refer to by short-hand throughout this case study as "WMD terrorism." In December 2002, in the midst of post-September 11 bureaucratic realignment, the President announced a national strategic policy on weapons of mass destruction.[19] The President called for the application of new technologies, increased emphasis on intelligence collection and analysis, the strengthening of alliance relationships, and the establishment of new partnerships with former adversaries. The main pillars of the President's program included interdiction efforts, nonproliferation programs, and consequence management. In particular, he called for an emphasis on improving intelligence regarding weapons of mass destruction facilities and activities, expanding the interaction among U.S. intelligence, law enforcement, and military agencies, and enhancing intelligence cooperation with friends and allies.[20]

High-level attention within the policy and intelligence communities has had an important impact on the WMD terrorism issue. Our interviews suggest that the Intelligence Community now has a more extensive operational capability dedicated to the problem, has enhanced its intelligence reporting and analysis functions, and has instituted a more robust effort to address the problem domestically. Moreover, the Community appears at least to recognize the unique characteristics of unconventional weapons in the terrorism context, as other organizations have followed the CIA's lead in placing additional—although not yet sufficient—resources for WMD terrorism into the counterterrorism effort.

Since September 11, the reallocation of resources to respond to WMD terrorism has resulted in significant improvements in both foreign and domestic intelligence. We understand that within the Intelligence Community, sources have gotten better, the amount of data available has dramatically increased, and intelligence is more harmonized, consistent, and less reliant on vague

"chatter." On the domestic side, there have been significant attempts to disrupt terrorist means of delivery.[21]

Despite all of these noteworthy developments, our study found that the Community still has a long way to go before it can claim to have optimized its counterterrorism capabilities or fully fixed the serious deficiencies that existed prior to September 11. We thus turn to the areas where the picture is not as promising.

We begin by focusing on needed improvements in the sharing of terrorism information with state, local, and tribal governments. Next, we examine the more general bureaucratic "turf war" between agencies, and the pronounced lack of clarity as to the roles, responsibilities, and authorities involving various entities tasked with the counterterrorism mission—particularly the NCTC and the Counterterrorist Center. Finally, we examine the continuing coordination problems between the CIA, FBI, and Homeland Security in addressing the threat posed by WMD terrorism.

INFORMATION SHARING: MUCH ROOM FOR IMPROVEMENT

Finding 1

Although terrorism information sharing has improved significantly since September 11, major change is still required to institute effective information sharing across the Intelligence Community and with state, local, and tribal governments.

For a number of years before the September 11 attacks, the Intelligence Community closely followed the al-Qa'ida terrorist threat, yet failed to adequately exploit information it had concerning several individuals who were either involved in the planning of or participated in the attacks.[22] Although the 9/11 Commission did not find that better information sharing would have prevented the attacks, at least nine of the ten "operational opportunities" that the commission identified as missed opportunities to possibly thwart the plot pertain to some form of a failure to share information.[23] These perceived failures have made "information sharing" a mantra for intelligence reform for the three and a half years since the attacks.

We have found that as a general matter, the Intelligence Community has sought to improve terrorism information sharing by modifying the structures and processes for sharing that were in place prior to September 11—rather than establishing wholly new approaches. We agree with the recent assessment of the Intelligence Community Inter-Agency Information Sharing Working Group, which found that "[a] great deal of energy…is being expended across the [Intelligence Community] to improve information sharing. However, the majority of these initiatives *will not produce the enduring institutional change required to address our current threat environment*."[24]

The importance of effective sharing of information at all levels of the Intelligence Community is discussed in several chapters of our report, but particularly in Chapters Nine (Information Sharing) and Eight (Analysis). In this section, we specifically address the Intelligence Community's efforts, since September 11, to improve the sharing of terrorism information across the Intelligence Community and with state, local, and tribal governments. Our specific findings are categorized in four broad areas.

First, we found substantial improvement in information sharing relating to terrorist watchlisting and screening. "Watchlisting"—the process of assembling databases of known or suspected terrorists—was not well coordinated among federal agencies prior to September 11, but several effective reforms have been implemented in the wake of the attacks.[25] For example, the new Terrorist Screening Center—an interagency effort to consolidate terrorist watchlists and provide operational support for federal employees around the world, 24 hours a day, seven days a week—now administers a single database that combines international and domestic terrorism data provided by the NCTC and FBI. The database also integrates information from immigration and customs offices, the Transportation Security Administration, the U.S. Marshals Service, Department of Defense, and Interpol. The Terrorist Screening Center ensures that government investigators, screeners, and agents are working from the same comprehensive information and that they have access simultaneously to information and experience that will allow them to act quickly when a suspected terrorist is screened and stopped.

Second, we have found that the sharing of counterterrorism information has increased in quantitative terms—more terrorism information is being shared with more entities both inside and outside the Intelligence Community than before the September 11 attacks. This has largely occurred through the

increased use of "tearlines"—the practice of generating intelligence reports at several different classification levels so it can be shared with a cross-section of federal, state, local, and tribal officials—which has resulted in more releasable information being provided to consumers.[26] And security-based sharing restrictions have been substantially reduced, allowing analysts and security personnel greater access to the information they need to do their jobs.[27]

All this being said, problems remain. While the Intelligence Community has reduced its use of restrictions on further dissemination of intelligence products without the consent of the originator,[28] inconsistent application of dissemination restrictions, such as ORCON ("originator controlled"), continue to impede the flow of useful terrorism information.[29] In relations with state, local, and tribal authorities, more terrorism information is being shared, but federal officials continue to have difficulty establishing consistent and coordinated lines of communication with these officials.[30] In this regard, we have found that there is no comprehensive policy or program for achieving the appropriate balance regarding what terrorism information to provide to state, local, and tribal authorities and how to provide it. Additionally, the redundant lines of communication through which terrorism-related information is passed—for example, through the Joint Terrorism Task Forces, Anti-Terrorism Advisory Councils, Homeland Security Information Network, TTIC Online, Law Enforcement Online Network, Centers for Disease Control alerts, and Public Health Advisories, to name just a few—present a deluge of information for which state, local, and tribal authorities are neither equipped nor trained to process, prioritize, and disseminate.

Our third category of findings relates to the sharing of information to ensure that analysts throughout the Intelligence Community have the widest possible access to information regardless of which agency collects the information. Today, the primary means of sharing information throughout the Community continues to be through interagency personnel exchange programs, such as the model used by the NCTC. These personnel exchanges can be quite effective, but they do nothing to improve the flow of information throughout those agencies or enable agencies to engage in competitive analysis based on access to the same set of information. Collectors of information continue to operate as though they "own" information and, in fact, collectors largely control access to the information that they generate. Decisions to withhold information are typically based on rules that are neither clearly defined nor consis-

tently applied, with no system in place to hold collectors accountable for inappropriately withholding information.

Finally, we have found that there is currently no single entity in the Intelligence Community with the responsibility and authority to impose a centralized approach to sharing information. Although the NCTC model has certainly facilitated improved information sharing on counterterrorism issues, it lacks sufficient authority and resources necessary to provide strong leadership in this area.

COUNTERTERRORISM WARNING AND ANALYSIS: A STRUGGLE BETWEEN AGENCIES

Notwithstanding significant gains in terrorism intelligence since September 11, a number of problems remain. Our study found evidence of bitter bureaucratic "turf battles" between agencies, and a pronounced lack of clarity as to the roles, responsibilities, and authorities of various entities tasked with the counterterrorism mission. Specifically, this interagency jockeying over overlapping counterterrorism analytical responsibilities indicates that major organizational issues affecting the allocation of resources, assignment of responsibilities, coordination of analysis, and effective warning remain unresolved.

Who's in Charge of Counterterrorism Analysis and Warning?

Finding 2

Ambiguities in the respective roles and authorities of the NCTC and CTC have not been resolved, and the two agencies continue to fight bureaucratic battles to define their place in the war on terror. The result has been unnecessary duplication of effort and the promotion of unproductive competition between the two organizations.

The Community's inability to implement a "one team, one fight" strategy in the terror war may be attributed both to ongoing bureaucratic battles between agencies charged with responsibility for counterterrorism analysis and warning, as well as the failure of Community leaders to effectively resolve these disputes and clearly define agency roles and authorities. The conflict and

ambiguity surrounding the role of the Terrorist Threat Integration Center during its abbreviated existence starkly illustrates both points.

After the September 11 attacks, TTIC was created for the purpose of improving the sharing of terrorist threat data and the analysis of terrorism-related information. However, as the Markle Foundation has reported, "the very fact of the TTIC's creation caused confusion within the federal government and among state and local governments" about the respective roles of TTIC and other federal agencies responsible for counterterrorism analysis and terrorist threat assessments.[31] Even today—despite being designated by the intelligence reform act as the preeminent, integrated center for threat warning and analysis—the NCTC continues to have difficulty asserting its primacy for the terrorism warning mission.

This dispute—and the potential problems to which it could lead—has been apparent since February 2003, when Senators Collins and Levin highlighted the issue in a joint letter (the "Collins-Levin Letter") to the Secretary of Homeland Security, the Director of TTIC, and the Directors of Central Intelligence and the FBI. The letter asked that the officials clarify responsibilities among counterterrorism elements of the U.S. government. In their April 2004 response, the agency heads stated that "TTIC has primary responsibility in the [U.S. government] for terrorism analysis (except analysis relating solely to purely domestic terrorism) and is responsible for the day-to-day terrorism analysis provided to the President and other senior policymakers."[32] In order to make it possible for TTIC to achieve this mission, the letter further stated that the DCI, in consultation with the other leaders of the Intelligence Community, would determine by June 1, 2004, what additional analytic resources would be transferred to TTIC from the CTC.[33]

Despite this unequivocal statement, TTIC was never able to fully perform its mission. Other entities, CTC in particular, differed over the level of support they should provide to TTIC and resisted supplying it with an adequate number of detailees—thus hampering TTIC's ability to assume the leading role assigned to it.

In May 2004, TTIC Director John Brennan sent correspondence to then-Director of Central Intelligence George Tenet, explaining how TTIC intended to carry out the responsibilities identified in the Collins-Levin letter. He warned that lacking significant new analytic resources, TTIC would not be

able to carry out the mission of having "primary responsibility" for providing terrorism analysis to the President and senior policymakers.[34]

The next month, Director Brennan sent the DCI a follow-up memorandum entitled "TTIC at the Breaking Point." In this memorandum, he argued that other intelligence agencies had failed to provide sufficient numbers of analysts to TTIC, and that the personnel that had been provided possessed only limited competency or a low level of experience. He further noted that these agencies continued to insist on developing their own independent counterterrorism analytical capabilities. This organizational multiplicity, Director Brennan argued, had created not only a "dangerous shortfall in TTIC's analytic resources and mission," but also "unnecessary analytic redundancy within the intelligence, law enforcement, defense, and homeland security communities."[35] In sum, Director Brennan wrote, a general refusal by entities within the Intelligence Community to "sign on to the fundamental premise that resources and mission will migrate to TTIC" had left the Center "unable to fulfill the mission of 'primary responsibility' for terrorism analysis in the U.S. government," and had forced the U.S. government into a "retreat from the integration model" of terrorism analysis and threat warning.[36]

Approximately one week later—on July 2, 2004—then-Deputy Director of Central Intelligence John McLaughlin attempted to address Director Brennan's concerns by outlining (at the DCI's request) a "division of resources and analytical responsibilities" between CIA and TTIC.[37] In interviews with this Commission, Director Brennan repeatedly stated that he had not received an official answer to his urgent memos of May and June.[38] When later asked specifically about the July 2 response, he dismissed it as failing to provide a meaningful answer to the basic questions he had raised regarding allocation of responsibilities for counterterrorism analysis and warning—despite the fact that the July 2 memorandum does in fact deal with virtually every issue highlighted by Director Brennan.[39]

The memorandum may not have been the answer Director Brennan wanted, but it certainly constituted a clear attempt by the Community's leadership to allocate roles, responsibilities, and resources among counterterrorism organizations. Addressed to CIA's Deputy Directors for Intelligence and Operations, as well as to Director Brennan, the memorandum provided for the immediate transfer of 60 personnel to TTIC, but it did not provide the "primary responsibility" over terrorism analysis for TTIC that Director Brennan had requested.

In fact, the memorandum declined to grant TTIC sole authority over analysis pertaining to international terrorist networks, instead explicitly stating that other agencies (including CTC) would continue sharing that function. The memorandum acknowledged that this would result in redundancy, but argued that "on something as important as terrorism analysis," some overlap between agencies was to be preferred.[40]

Although we believe that excessive redundancy in Community counterterrorism efforts is wasteful of scarce resources and thus counterproductive (see our discussion below), we express no view on the overall merits of the organizational plan and division of labor outlined in the July 2, 2004 memorandum. However, it is of great significance, we think, that the Community was ultimately unable to enforce that plan—or, to date, *any* plan—and bring an end to the interagency squabbling between CTC and NCTC.

We have been told that the plan outlined in the July 2 memorandum fell victim to bureaucratic neglect and rapid change within the Community; shortly after its distribution there was turnover in the DCI's office, and ambiguities fostered by creation of the NCTC by executive order and, later, passage of the intelligence reform act, raised new questions about the designated roles of the nation's counterterrorism organizations. Our study suggests that there may have been another factor, as well: the entrenched opposition of both CTC and NCTC to effectively cooperating or consolidating aspects of their authorities.

The fact that Director Brennan did not regard clear direction from the DCI to be an "answer" to his pleas to resolve confusion over roles, resources, and responsibilities—presumably because it did not allocate the prerogatives to his organization that he had requested—speaks volumes about the hardened mindsets of the two organizations' leadership, and their desire to protect or expand their bureaucratic "turf." As the Director of the Counterterrorist Center characterized the relationship, the Center "is fighting a war with TTIC." [41]

Although recent passage of the intelligence reform act may resolve issues related to responsibilities and resources,[42] the history of the dispute tempers our optimism. Whatever the precise allocation of resources and responsibilities is to be, the DNI must act quickly to resolve the issue. Absent strong leadership, other organizations in the Intelligence Community may continue to resist providing resources to NCTC, as they did with TTIC, and may dispute its "primary" role in coordinating terrorism intelligence.[43] Alternatively,

NCTC may resist well-reasoned direction to permit CTC to continue performing several of its important functions. If so, the war between agencies that are tasked to fight the war on terror will continue. Unfortunately, such a conflict constitutes far more than a common bureaucratic dispute, the sort of administrative power struggle so common in the corridors of government. Rather, it has profound operational implications for the ability of the Intelligence Community to perform the all-important function of providing terrorism analysis and warning information to policymakers.

A Failure to Warn with One Voice

Finding 3

Persisting ambiguities and conflicts in the roles, missions, and authorities of counterterrorism organizations hamper effective warning.

The dispute between the NCTC and CTC is especially troubling in the context of threat warning—the process by which threat information is conveyed to decisionmakers in time for them to take action to manage or deter the threat. Continuing disagreements about the two offices' roles and missions have in the past led to inconsistent warning messages being conveyed to decisionmakers and—far more troubling—these warnings were conveyed in a manner that may have sowed confusion.

What Part of "Warning" Should Be Competitive?

For present purposes, we divide warning into two components: (1) the *analytic* function that produces a warning and (2) the *process of communicating* those threat judgments to decisionmakers. As a general matter, while we strongly endorse competitive *warning analysis* (*i.e.*, competition in the first component of warning), we believe that the process of communicating threats to decisionmakers (*i.e.*, the second component) should be coordinated and integrated. We say this because we do not believe decisionmakers are well-served by incoherent, uncoordinated warnings of impending threats. Rather, warning should be presented to decisionmakers in a coordinated manner that makes clear the level of certainty with which they are held.

According to NCTC officials, the NCTC must have primacy, if not exclusivity, in providing warning intelligence to the President and controlling the analytical resources required for this mission.[44] NCTC principals acknowledge that CTC needs to retain analytical capability to directly support the CIA's Directorate of Operations (DO)—and to continue the spectacular successes the DO has achieved in the war on terror.[45] However, as a general matter they assert that it is improper to "divide effort when it comes to terrorism,"[46] and have claimed as a core responsibility the "production of terrorist threat warnings, advisories, and alerts," which are to be "issued by [the NCTC] alone or as formally coordinated products of the 'Warn 7.'"[47] Moreover, in its role as coordinator of the President's Terrorist Threat Report (PTTR), the NCTC insists that it has oversight responsibility for determining what terrorism analysis is provided to the President.[48] In sum, the NCTC conceives its mission as providing coordinated threat warning and analytical reports—reflecting "diversity of viewpoint but coordination of common response"—to senior policymakers.[49]

Perhaps unsurprisingly, CTC does not embrace this division of labor. CTC views itself as the preeminent counterterrorism entity within the Intelligence Community.

In CTC's view, NCTC's main contribution to the terrorism fight lies in its access to intelligence information and databases—both foreign and domestic.[50] As a result, CTC leaders expressed to us the view that the NCTC should be responsible for generating an integrated Community view of threats, but should *not* have the dominant voice in counterterrorism analysis and warning.[51] A recent example of where this theoretical disagreement had concrete consequences is discussed in our classified report, but cannot be detailed in an unclassified format.

Ideally, a single warning vehicle (such as the President's Terrorist Threat Report, now provided daily by the NCTC) should provide a forum for ensuring that policymakers do not receive inconsistent messages. But we have seen evidence that this is not always so. It is further possible that legislation creating the NCTC may obviate such interagency conflicts in the future—but we are only guardedly optimistic.[52] In this sense, we believe that the DNI will have to create mechanisms by which competitive analysis for warning is maintained, and the dissemination of warnings is carefully coordinated. We address this issue more fully in Chapter Eight of our report (Analysis). More

broadly, the DNI will have to force the nation's counterterrorism organizations to concentrate more fully on fighting terrorists, rather than each other.

Maintenance of Redundant Capabilities

Finding 4

Persistent ambiguities and conflicts in the roles, missions, and authorities of counterterrorism organizations with regard to analysis and warning have led to redundant efforts across the Community and inefficient use of limited resources.

An absence of clearly defined roles and authorities with regard to analysis and warning leads inevitably to competition in key capabilities, and redundant efforts across the Community. For example, we spoke with a senior analytic manager who recounted one incident in which a single raw intelligence report spurred five different agencies to write five separate pieces, all reaching the same conclusion. Not only were analysts' efforts redundant, but policymakers were then required to read through all five papers to look for subtle differences in perspective that could have been better conveyed in a single, coordinated paper.[53]

This phenomenon is especially troubling given the scarce analytic resources available for counterterrorism efforts. Agencies expressed serious concern about their ability to engage in long-term strategic analysis given the demands generated by customer questions and daily indicators of new threats.[54] For example, the NCTC spends roughly 70 percent of its time on immediate threats,[55] primarily because analysts have to run each potential threat to ground, even if it seems suspect from the outset.[56] Similarly, the FBI estimates that about 50 percent of analysts' time is spent on direct operational support.[57] All of these requirements tend to leave little time and resources for thoughtful, strategic work on new and emerging threats. All of this is, of course, compounded by the significant trouble agencies are experiencing in retaining qualified and experienced analysts.[58]

Despite this serious resource issue, there is ongoing evidence of an interagency failure to cooperate and efficiently divide responsibility in counterterrorism analysis. For example, NCTC WMD analysts with whom we spoke described their willingness and capability to engage in long-term, strategic analysis on behalf of

the counterterrorism community.[59] But when a senior CTC official—who noted the need for such analysis and lamented the difficulty of allocating time and resources for it in the context of CTC's operationally-driven environment—was asked about the possibility of using NCTC resources for that purpose, he stated bluntly that "[NCTC] doesn't have those capabilities."[60] It is unclear whether such statements reflect a lack of understanding between the two entities concerning complementary capabilities that could be mutually leveraged, institutional resentment and an unwillingness to operate collaboratively, or simply an ongoing struggle over personnel resources.

Again, although recent passage of the intelligence reform act may resolve issues related to responsibilities and resources,[61] we are not optimistic that anything in the legislation itself resolves the dispute. We address the issues associated with managing scarce analytic resources more fully in Chapters Six (Leadership and Management) and Eight (Analysis).

THE FAILURE TO MANAGE COMMUNITY RESOURCES IN RESPONSE TO THE WMD TERRORISM THREAT

Finding 5

The failure to manage counterterrorism resources from a Community perspective has limited the Intelligence Community's ability to understand and warn against terrorist use of weapons of mass destruction.

Recognizing that the worst terrorist attack would be one involving weapons of mass destruction, some elements within the Community have begun to incorporate analytic and collection capabilities with respect to the WMD terrorism threat into their counterterrorism organizations. At the same time, the CIA's Weapons Intelligence, Nonproliferation, and Arms Control Center provides intelligence support aimed at protecting the United States and its interests from all advanced weapons threats. Our review of the relationship among these various entities reveals that some systemic weaknesses are preventing the development of a focused, integrated, well-resourced bureaucracy that can most effectively combat the worst-case threat of a homeland terrorist attack. Specifically:

- There is no clear leadership or bureaucratic architecture defining roles and responsibilities for WMD terrorism. This adversely affects analysis, collection, and threat warning; and

- The domestic intelligence effort on WMD terrorism is lagging behind the U.S. government's foreign intelligence capabilities.

Defining Roles and Responsibilities for the WMD Terrorism Threat

Notwithstanding the President's National Strategy to Combat Weapons of Mass Destruction promulgated in December 2002, the overriding concern of key officials whom we have interviewed is that, within the U.S. government, there is no overall direction and coordination on WMD terrorism. As the chief of the FBI's WMD Countermeasures Unit rhetorically asked, "[w]ho is ultimately responsible for preventing the use of a WMD?" [62]

The most significant consequence of the lack of coordination is that each organization appears to be defining its own mission and trying to make sure it has the resources to be self-sufficient across a broad range of responsibilities.[63] The result is predictable: duplicative roles, power vacuums where individual organizations assert their authority, and confusion within the Community. As the NCTC's head of analysis observed, it is necessary not only to clarify affirmative roles and responsibilities, but also to delineate those responsibilities for which agencies are *not* responsible.[64]

For example, despite changes since September 11, coordination problems between the FBI and the CIA continue to disrupt analysis on WMD terrorism and operations against weapons of mass destruction targets. As the FBI has expanded its overseas operations and the CTC tries not to lose its targets when they travel to the United States, coordination is essential. However, according to the head of the CTC's WMD unit, there is no sense of "jointness," or shared mission, on the part of the FBI and CTC, despite the co-location of portions of both organizations.[65]

It appears that coordination among domestic agencies responsible for responding to a potential WMD terrorist threat also suffers from confusion and a lack of coordination. For instance, the FBI told us that the Department of Homeland Security had, in response to a possible threat, taken the initiative to start moving radiation detection resources to New York during the Republi-

can National Convention without coordinating with the Bureau. Subsequent to the move, the "threat" was revealed to be a legitimate movement of a medical isotope.[66] Had even the most elemental communication and coordination taken place—in the form of a phone call from Homeland Security to the FBI—this fact might have surfaced earlier, thereby avoiding the squandering of limited counterterrorism resources.[67]

Perhaps most alarming is the allegation that when terrorism cases move from a purely foreign focus to a domestic emphasis requiring a hand-off in primary responsibility from the CIA to the FBI, the CIA finds it difficult to obtain information from the FBI about ongoing investigations.[68] Such gaps in cooperation, occurring at the vital fault line between foreign and domestic intelligence, are reminiscent of the "void" that the September 11 attack plotters operated in to achieve their objectives.[69]

The stark division between the Intelligence Community's WMD terrorism programs and the Community's state-based weapons of mass destruction programs further hampers the WMD terrorism effort.[70] As our case study of al-Qa'ida in Afghanistan also confirms, the personnel who work the WMD terrorism issue mostly coordinate with their state program counterparts on an *ad hoc* basis. Efforts have been made to remedy this problem within CIA,[71] but we think it vital that such cooperation be greatly expanded throughout the Community.

The Domestic Intelligence Effort on WMD Terrorism

While the FBI has responded to the threat posed by WMD terrorism by increasing the resources dedicated to this issue, the FBI's efforts in this regard remain subordinated to the broader war on terror. For example, approximately a year ago, the FBI committed (on paper) to staffing its WMD Integration and Targeting Unit—the unit responsible for providing expertise on WMD terrorism—with a total of 26 staff positions. Today, the unit has only two people—the unit chief and a single intelligence analyst.[72]

Unsurprisingly, the FBI, like other agencies responsible for the WMD terrorism threat, is having difficulty finding people with the right expertise and has yet to develop a specific career track or program for developing expertise regarding the threat.[73] Other agencies having responsibility for WMD terrorism are also understaffed, and the few experts that do exist are suffering from

burnout.[74] To its credit, the FBI has acknowledged its need for more resources in this area,[75] but it is clear to us that the FBI's weaknesses are not susceptible to a quick fix. We discuss our proposals addressing this and related issues more fully in Chapters Six (Leadership and Management), Eight (Analysis), and Ten (Intelligence at Home).

CONCLUSION

The Intelligence Community's capabilities with regard to current terror threats have improved significantly since September 11, 2001. Nevertheless, the continued lack of definitional clarity as to roles and responsibilities in the war on terrorism, and ongoing conflicts among key counterterrorism agencies, constitute an ongoing challenge—and one that we believe should be foremost on the mind of the new DNI.

ENDNOTES

[1] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (2004) (hereinafter "9/11 Commission Report") at p. 353.

[2] *Id*. at p. 371.

[3] *Id*. at pp. 277, 408-09.

[4] Eleventh Public Hearing of the National Commission on Terrorist Attacks Upon the United States, *Staff Statement Number 11* (April 14, 2004) at p. 3.

[5] *Id*. at p. 5.

[6] 9/11 Commission Report at p. 263.

[7] Interview with Terrorist Screening Center official (Nov. 9, 2004).

[8] Interview with TTIC senior officials (Oct. 19, 2004); Interview with DIA (JITF-CT) analysts (Oct. 26, 2004); Interview with Department of State (INR) analysts (Nov. 3, 2004).

[9] NCTC was created on December 6, 2004 pursuant to Executive Order. The establishment of NCTC is also codified by the *Intelligence Reform and Terrorism Prevention Act of 2004* (hereinafter "IRTPA"). Under IRTPA, NCTC subsumes the primary duties of TTIC, and is intended to serve as the governmental entity responsible for counterterrorism analysis and warning and for developing strategic operational plans for counterterrorism operations conducted by the U.S. government. Nevertheless, although the name has changed, the organization and its bureaucratic challenges remain essentially the same, and the identical problems surrounding TTIC that are discussed in this report threaten to envelope the newly-created NCTC. In this report, for ease of reference, when we use the term NCTC, we refer to both NCTC and its predecessor, TTIC, unless otherwise noted.

[10] Interview with TTIC senior analyst (Nov. 5, 2004).

[11] Interview with TTIC (WMD) analysts (Oct. 19, 2004).

[12] *Id*.

[13] Interview with TTIC senior analyst (Oct. 19, 2004); Interview with TTIC senior analyst (Nov. 5, 2004).

[14] Along with NCTC, these agencies have been dubbed the "Warn 7." Interview with TTIC senior analyst (Oct. 19, 2004).

[15] Interview with TTIC senior analyst (Oct. 19, 2004). During the "Summer of Threat" prior to the September 11 attacks, the interagency Counterterrorism Security Group (CSG), headed by Richard Clarke, had access to disseminated intelligence from several agencies, but it did not have the capability to integrate intelligence from each agency on a daily basis, nor did it have access to the internal, non-disseminated information of intelligence agencies. 9/11 Commission Report at p. 255.

[16] Interview with NCTC senior official (Feb. 4, 2005); Interview with TTIC senior analyst (Oct. 19, 2004); Interview with TTIC senior analyst (Nov. 5, 2004).

[17] The PTTR is produced six days a week, usually runs three to five pages in length, and may have, on average, one to four articles. It is delivered to the President and senior policymakers by the PDB briefers. Interview with TTIC senior analyst (Nov. 5, 2004).

[18] Interview with CTC (WMD) official (Oct. 22, 2004).

[19] National Security Presidential Directive 17, *National Strategy to Combat Weapons of Mass Destruction* (Dec. 2002).

[20] *Id*.

[21] Interview with FBI (WMD) officials (Oct. 14, 2004); Interview with FBI (Counterterrorism) official (Oct. 22, 2004).

[22] The 9/11 Commission identifies several instances in which sharing of information might have led to further investigation that could have revealed the plot, but does not conclude that the sharing of any specific pieces of information actually held would have likely led to preventing the attacks. *See, e.g*., 9/11 Commission Report at pp. 272, 276.

[23] *Id*. at pp. 355-356.

[24] *Calibration Report: Intelligence Community Collaboration and Information Sharing to Win the War on Terrorism: Phase 1* (May 2004) at p. ES-1 (hereinafter "IC Inter-Agency ISWG May 2004 Calibration Report") (emphasis in original).

[25] These watchlisting reforms were undertaken at the direction of the President, primarily under Homeland Security Presidential Directive 6, *Integration and Use of Screening Information* (Sept. 16, 2003).

[26] This finding is consistent with the conclusion of the Inter-Agency Information Sharing Working Group. *FY2004 Congressionally Directed Actions on Information Sharing, Consolidated Report of the Information Sharing Working Group* (Dec. 14, 2004) at p. 23.

[27] Interview with TTIC senior analyst (Oct. 19, 2004); Interview with TTIC senior official (Oct. 19, 2004); Interview with DIA (JITF-CT) analysts (Oct. 26, 2004); Interview with State Department (INR) analysts (Nov. 3, 2004); Interview with FBI (National Joint Terrorism Task Force) official (Nov. 5, 2004); Interview with CIA (DO) official (Nov. 8, 2004).

[28] Interview with TTIC senior official (Oct. 19, 2004); Interview with DIA (JITF-CT) analysts (Oct. 26, 2004). Between 2001 and 2003, the rate of use of originator controls on terrorism-related reporting across the Intelligence Community dropped by approximately 50 percent. Seventh Public Hearing of the National Commission on Terrorist Attacks Upon the United States (Jan. 26, 2004) (Statement of Russell E. Travers, TTIC Deputy CIO for Information Sharing).

[29] The rule of originator control, or ORCON, allows the agency that originates information to retain control over its dissemination and declassification (if it is classified) or its release to non-governmental parties. *See, e.g*., IC Inter-Agency ISWG May 2004 Calibration Report, NRO submission, Appendix B at p. B-37 (listing ORCON as a cultural barrier that "must…be addressed"); *id*., DIA submission, Appendix B at p. B-12 (citing FBI and NSA ORCON dissemination as constraining assembly of terrorism intelligence database).

[30] Interview with CIA (Collection Concepts Development Center) official (Oct. 7, 2004); Interview with FBI (WMD) officials (Oct. 13, 2004); Interview with emergency preparedness official of the Office of the Governor of Virginia (Nov. 10, 2004); Homeland Security Advisory Council, *Final Report: Intelligence and Information Sharing Initiative* (Dec. 2004).

[31] Markle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Information Network for Homeland Security* (2003) at pp. 7-8. The Markle Foundation funds a variety of studies that analyze the potential of new technologies to address critical public sector needs, particularly in the areas of health and national security.

[32] Letter from Thomas J. Ridge, Secretary of Homeland Security; Robert S. Mueller, III,

Director Federal Bureau of Investigation; George J. Tenet, Director of Central Intelligence; and John O. Brennan, Director Terrorist Threat Integration Center; to The Honorable Susan M. Collins, Chairwoman Senate Committee on Governmental Affairs, and The Honorable Carl Levin, Ranking Member (Apr. 13, 2004) at p. 2.

[33] *Id*.

[34] Memorandum from John O. Brennan, TTIC Director, to Director of Central Intelligence (May 19, 2004) at pp. 2-4, 6-8.

[35] Memorandum from John O. Brennan, TTIC Director, to Director of Central Intelligence (June 23, 2004).

[36] *Id.*

[37] Memorandum from John E. McLaughlin, Deputy Director of Central Intelligence (July 2, 2004).

[38] Interviews with John O. Brennan, TTIC Director (Sept. 22, 2004 and Feb. 8, 2005).

[39] Interview with John O. Brennan, Interim Director of NCTC (March 15, 2005). The July 2 memorandum does not directly discuss the counterterrorism responsibilities of FBI, DHS or the Defense Department, which are mentioned briefly in Director Brennan's first memorandum.

[40] *Id*.

[41] Interview with Director of CTC (Nov. 5, 2004). Other CTC personnel expressed the same sentiment, using nearly identical language. Interview with senior CTC official (Oct. 22, 2004).

[42] IRTPA at § 1021 (adding section 119 to the National Security Act to establish the NCTC in law, provide its primary missions, and outline the reporting chain of its director).

[43] *Id*. at § 1021 (adding section 119(d) to the National Security Act to provide that one of the primary missions of the NCTC is to "serve as the primary organization in the United States Government for analyzing and integrating all intelligence…pertaining to terrorism").

[44] *See, e.g.*, Interview with TTIC senior official (Feb. 4, 2005).

[45] Interview with TTIC senior analyst (Oct. 19, 2004).

[46] Interview with TTIC senior official (Feb. 4, 2005).

[47] NCTC, CIA, FBI, DIA, NSA, and the Departments of State and Homeland Security comprise the so-called "Warn 7." *Id*.; Memorandum from John O. Brennan, TTIC Director, to Director of Central Intelligence (May 19, 2004) at ¶ 7.

[48] Letter from Thomas J. Ridge, Secretary of Homeland Security; Robert S. Mueller, III, Director Federal Bureau of Investigation; George J. Tenet, Director of Central Intelligence; and John O. Brennan, Director Terrorist Threat Integration Center; to The Honorable Susan M. Collins, Chairwoman, Senate Committee on Governmental Affairs, and The Honorable Carl Levin, Ranking Member (April 13, 2004) at p. 3; IRTPA at § 1021(f)(D).

[49] Interview with TTIC senior analyst (Oct. 19, 2004).

[50] Under IRTPA, NCTC serves not only as the governmental entity responsible for counterterrorism analysis and warning, but is also responsible for developing strategic operational plans for counterterrorism operations conducted by the U.S. government. It is our understanding that details regarding how NCTC will perform its strategic operational planning role have not fully been resolved. Accordingly, this report does not address NCTC's responsibility for this strategic planning function. IRTPA at § 1021.

[51] Interviews with CTC senior officials (Oct. 22, 2004 and Nov. 5, 2004).

[52] The law vests the NCTC with authority to "disseminate terrorism information, including current terrorism threat analysis," to senior policymakers, but does not grant it exclusive authority to do so. Moreover, the NCTC is given "primary responsibility within the United States Government for conducting net assessments of terrorist threats." But the law also states that nothing in its text "shall limit the authority of [other agencies] to conduct net assessments." IRTPA at §§ 1021(f)(1)(G), 1021(f)(2).

[53] Interview with FBI (Counterterrorism) official (Nov. 4, 2004).

[54] Interview with CTC official (Oct. 22, 2004); Interviews with TTIC senior analyst and TTIC (WMD) analysts (Oct. 19, 2004); Interview with DIA analysts and managers (Oct. 26, 2004); *see also* Interviews with former senior Intelligence Community officials (Sept. 28, 2004 and Oct. 15, 2004).

[55] Interview with TTIC senior analyst (Oct. 19, 2004).

[56] Interview with TTIC (WMD) analysts (Oct. 19, 2004).

[57] Interview with FBI (Counterterrorism) official (Nov. 4, 2004).

[58] CTC cited burnout as a critical retention problem. Interview with CTC (WMD) official (Oct. 22, 2004). DIA cited examples of analysts leaving to work fewer hours for higher salaries with contractors. Interview with DIA analysts and managers (Oct. 26, 2004).

[59] Interview with TTIC (WMD) analysts (Oct. 19, 2004).

[60] Interview with senior CTC official (Oct. 22, 2004).

[61] IRTPA at § 1021.

[62] Interview with FBI (WMD) officials (Oct. 14, 2004). *See also* Interview with former senior intelligence official (Oct. 15, 2004) (discussing Collection Concepts Development Center (CCDC) study on the active interdiction of weapons of mass destruction, which underscored that one of the main underlying problems was that no one owned the problem of WMD terrorism); Interview with CTC (WMD) official (Oct. 22, 2004) (suggesting dedicating a NSC policy staffer to the issue); Interview with FBI (Counterterrorism) official (Oct. 22, 2004) (noting how the pre-election threat is an example of how U.S. government lacks a national WMD terrorism strategy).

[63] Interview with FBI (WMD) officials (Oct. 14, 2004).

[64] Interview with TTIC senior analyst (Oct. 19, 2004).

[65] Interview with CTC (WMD) official (Oct. 22, 2004); Interview with FBI (WMD) officials (Oct. 14, 2004).

[66] Interview with FBI (WMD) officials (Oct. 14, 2004).

[67] *Id*.

[68] Interview with CTC (WMD) official (Oct. 22, 2004); Interview with FBI (National Joint Terrorism Task Force) official (Nov. 5, 2004).

[69] 9/11 Commission Report at p. 263.

[70] Even the two groups' jargon differs. Those working on state-based programs talk of "WMD;" while those working on terrorism programs talk of "CBRN" (i.e., chemical, biological, radiological, and nuclear devices).

[71] An example of positive coordination is provided in our classified report, but cannot be discussed in an unclassified format.

[72] Interview with FBI (WMD) officials (Dec. 2, 2004).

[73] *Id.*
[74] *See, e.g.*, Interview with CTC (WMD) official (Oct. 22, 2004).
[75] Interview with FBI (WMD) officials (Oct. 14, 2004).