Intelligence Sharing:

Getting the National Counterterrorism Analysts on the Same Data Sheet

Colonel Daniel Putbrese
U.S. Air Force
Atlantic Council Senior Fellow

Occasional Paper
October 2006

THE ATLANTIC COUNCIL

OF THE UNITED STATES

The Atlantic Council promotes constructive U.S. leadership and engagement in international affairs based on the central role of the Atlantic community in meeting the international challenges of the 21st century. The Council embodies a nonpartisan network of leaders who aim to bring ideas to power and to give power to ideas by:

- stimulating dialogue and discussion about critical international issues with a view to enriching public debate and promoting consensus on appropriate responses in the Administration, the Congress, the corporate and nonprofit sectors, and the media in the United States and among leaders in Europe, Asia and the Americas;

- conducting educational and exchange programs for successor generations of U.S. leaders so that they will come to value U.S. international engagement and have the knowledge and understanding necessary to develop effective policies.

Table of Contents

Author's Note

As a twenty-year career Air Force intelligence officer, I was assigned in 2003 to the Joint Intelligence Task Force Combating Terrorism (JITF-CT). JITF-CT is the Department of Defense's (DoD) national level counterterrorism center, and this paper is dedicated to the men and women who serve there. During my tenure, I became extremely impressed with the dedication, patriotism, and intellect of the individuals who make up the organization. I witnessed analysts day after day trying to do their part to uncover terrorists and terrorist plots, despite the lack of access to all the data that the U.S. government had at its disposal. DoD's counterterrorism (CT) analysts are not alone; the CT centers at the State Department, Department of Homeland Security (DHS), National Security Agency (NSA) and the Federal Bureau of Investigation (FBI), also lack access to some or all of the unreported terrorism data required to work effectively with the Central Intelligence Agency (CIA) and the National Counter Terrorism Center (NCTC). Each of these CT centers has incredible talent and analytical firepower that is underutilized due to this lack of access. The grave concern over intelligence that goes undisseminated has been highlighted in the reports of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) and the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission), as well as in the Intelligence Reform Terrorism Prevention Act (IRTPA) and a report published by the Markle Foundation. *Yet, little has changed to get national level CT analysts access to unreported terrorism information.*

I hope this paper will provide recognition of the fact that national level CT centers continue to lack access to terrorism data and that resistance to sharing this data is so strong that much more far-reaching actions are required than those already made in response to the formal recommendations made by the commissions. In addition, I will put forth specific steps to be taken and delineate why progress must then be constantly monitored and modified to keep up with the circumvention that will inevitably follow.

My fellowship this past year at the Atlantic Council enabled me to step back and reflect on the profound significance of the lack of equal access to terrorism data. The time and resources afforded to me gave me the opportunity to interview over forty people, most of whom are current or retired high-level government officials that either are or were stakeholders in the information access debate. My interviewees included two retired CIA Directors, a retired FBI Director, a retired Chief Counsel for DoD, a retired CIA Deputy Director for Intelligence, the first NCTC Director (now retired), the current heads of information sharing at the NCTC, DHS, and DoD, the current DIA Chief of Staff, the current Director of the JITF-CT along with JITF-CT's Legal Counsel, and three senior Capitol Hill staffers from the House and the Senate. Moreover, I gained keen insights from senior analysts at DIA, CIA, DHS, NCTC, and FBI who struggle with these issues in the trenches every day. I made a concerted effort to understand the views of those with whom I initially disagreed, endeavored to keep an open mind and to appreciate all sides of the issue. Unfortunately, in some cases this proved very difficult, as I myself became a victim of some of the historic roadblocks put in place by some who want to thwart any attempt to take data access decisions away from those who now control it. This was exemplified on one occasion when my interview with a current CIA Reports officer was suddenly canceled the day it was to take place. The reason given was that when the news of my

research and planned visit reached some superiors, the Reports officer was directed not to talk to me.

Notwithstanding this and similar experiences, I feel confident that I was able to obtain a thorough understanding of opposing viewpoints. I fully appreciate the need to protect sources and methods and the consequences of having sensitive information fall into the wrong hands. I have become, however, even more concerned that collectors of data are not allowing other agencies working the same problem-set access to their data by invoking the need to prevent unauthorized disclosures. *There is no doubt that the United States needs to do a better job safeguarding its secrets, but to use that as an excuse to keep data from those who have a "true need to know" has the direct effect of putting national security in jeopardy.* This is continuing to happen despite the attention to this problem brought by the 9/11 and WMD Commissions. *The unavoidable conclusion is that the U.S. government cannot continue to allow a collecting agency to make unilateral originator control determinations regarding the intelligence it collects.* This is not to say that the collectors are not dedicated to stopping terrorist acts – they are totally dedicated. In my view, the country will never know the depth of their contributions to U.S. national security. With that said, I hope to explain why they are not in position to make the best "need to know" determinations – that decision must be made by an independent body.

The Office of the Director of National Intelligence (ODNI) is in the process of taking on the daunting challenges of creating an Information Sharing Environment (ISE) throughout all levels of government as mandated in the IRTPA. *It is absolutely imperative that the ISE architecture provide for equal access to terrorism data among the U.S. national CT centers.* Failure to do so will undoubtedly lead to loss of life that could have been prevented had these organizations been optimized together as an intelligence enterprise. It will not be easy to break down the bureaucratic walls and misguided protectionism that contribute to the resistance to intelligence sharing, but it must be done and it can be done in a properly secured network that takes into account what could happen should this valuable data fall into the wrong hands.

Intelligence Sharing

Getting the National Counterterrorism Analysts on the Same Data Sheet

Introduction

The 9/11 Commission's much celebrated and often cited report identified the resistance to intelligence sharing as "the biggest impediment to all source analysis – to a greater likelihood of connecting the dots."[1] There is broad agreement that intelligence sharing needs to be improved, but there is very little agreement on exactly what information should be shared, who it should be shared with, and how exactly the sharing should be accomplished. Perspectives on this issue vary greatly, ranging from those who argue the problem was solved by the creation of the NCTC, to those who contend that the problem is worse than ever and will never be solved because of characteristics inherent to the intelligence community (IC) that create impediments to intelligence sharing. Intelligence sharing is a complex issue, covering a multitude of different categories of information and intelligence that need to be shared horizontally and vertically among all agencies and between all levels of the U.S. government.

This paper will focus on one very important aspect of the overall information sharing quandary – the current failure to provide national counterterrorism (CT) centers access to undisseminated intelligence data required for the intelligence community to collaborate on stopping terrorists and their acts. This paper will discuss the national CT centers which make up the Interagency Intelligence Committee on Terrorism (IICT), specifically define the data access they require, explain why they require it, and the obstacles to their obtaining it. In addition, this paper will confront the arguments of those who are against this type of access, lay out what is required to achieve it, and then address potential circumvention that must be guarded against once a workable solution is in place.

It is imperative that the national CT centers be able to access undisseminated CT data at its earliest point of consumability-before it has been analyzed, filtered, and/or packaged. All source analysis is at its best when the data being analyzed is free of the ambiguities that set in once it is subject to human interpretation. *To achieve this goal, agencies that collect terrorism related intelligence must give up ownership of that data to an independent higher authority.* That authority needs not only to ensure that data is shared but must ensure equal access to that data. The WMD Commission report begins its chapter on information sharing with this very point:

[1] The 9/11 Report, *The National Commission on Terrorist Attacks Upon the United States*, St. Martin's Press, August 2004, 592 (hereinafter "9/11 Report").

> *"We begin with an important reservation about terminology. The term information 'sharing' suggests that the federal government entity that collects the information 'owns' it and can decide whether or not to 'share' it with others. This concept is deeply embedded in the intelligence community's culture. We reject it. Information collected by the intelligence community, or for that matter, any government agency, belongs to the U.S. government. Officials are fiduciaries who hold the information in trust for the nation. They do not have authority to withhold or distribute it except as such authority is delegated by the President or provided by law. As we have noted elsewhere, we think the Director of National Intelligence could take an important, symbolic first step toward changing the intelligence community's culture by jettisoning the term 'information sharing' itself – perhaps in favor of the term 'information integration' or 'information access.' But as the term 'information sharing' has become common practice parlance, we will use it in this chapter to avoid confusion."*[2]

This author could not agree more. The whole concept of CT centers having to ask for information needs to be abandoned. Lack of access will not be solved if human beings have to think whom to share with. A higher authority, independent of individual agencies, is required to control access to the data. That authority needs to designate offices within the intelligence community that qualify for raw and other unreported data by having mandated warning or offensive terrorism missions along with a capacity to consume, evaluate, analyze, and/or collaborate on that intelligence. The Intelligence Reform and Terrorism Prevention Act (IRTPA) provides the Office of the Director of National Intelligence (ODNI) the authority to make this a reality. It is essential, if future terrorist attacks are to be prevented, that the agencies that make up the so-called "intelligence community" act as an integrated enterprise. Until national CT analysts have equal access to terrorism data, sorely needed manpower and expertise currently dispersed throughout the national CT community, will not be optimally focused. The United States needs the cumulative power of all the analytical minds that make up the national CT centers in order to coalesce the invaluable analytical perspectives that emerge from each agency's unique roles, missions and culture.

Recognition of this need did not begin on September 11, 2001. The issue has been with the IC since its inception. In 1982, in the aftermath of the kidnapping of Brigadier General James Dozier, President Reagan asked William Casey, the Director of the CIA, to improve interagency intelligence sharing to better combat terrorism. The result was the creation of the Interagency Intelligence Committee on Terrorism (IICT). This Committee created a national terrorism warning mechanism that included the coordination and collaboration of CT analysts within the State Department, Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), National Security Agency (NSA), and the Federal Bureau of Investigation (FBI). Following the attacks of September 11, 2001 (9/11) the Department of Homeland Security (DHS) and the NCTC were created, bringing the number of agencies that make up the IICT to seven.[3] Today, under the leadership of the NCTC, the IICT coordinates and collaborates on community terrorism assessments and a wide range of warning products that have evolved into an Intelligence Community Terrorist Threat Warning System. The process has evolved well, except for one fundamental flaw: members do not have equal access to

[2] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President of the United States, March 2005, 430.

[3] From this point forward this paper will refer to the seven CT centers that are members of the IICT as the "national CT centers."

terrorism information. Before providing a rationale for granting such access, it may first make sense to describe just what "data access" actually means.

CT Data Access Defined

Analysts in the national CT centers have access to the NCTC's homepage with special access to read the NCTC daily terrorist threat summary. Each center has individuals in leadership positions that sit in the daily morning and afternoon Video Teleconferences (VTC) to discuss known threats that are in "reported information." Communications between the national CT centers, although improved since 9/11, are still almost exclusively related to reported information. Discussion of unreported information is almost nonexistent. On the rare occasions when it does occur, it is usually above the analyst level and the discussion is centered on data considered by the participants as "sexy." Yet, what is needed to connect the dots is analysts with access to the unassuming data that has not been determined to be significant and may never be revealed or evolve unless enough of the national CT analysts have an opportunity to access and assess it. Agencies that control access to their collected data will make a case that information is shared better than ever and opportunities to coordinate and collaborate are vastly improved. *The problem is they will only be referring to the reported information, as access to unreported information has not changed for the five national CT centers that do not have access.* Unreported data can take on many forms but, for the purposes of this paper, the term is used to describe primarily the following four categories of CT information.

CIA Operations Cables: Intelligence Masquerading as Operational Data

These cables are the operational (ops) reports to and from the field that have massive amounts of data but do not make it into CIA disseminated reporting. The cables give keen insights into the kind of access the source of the information had (for example, was he Saddam Hussein's body guard or a friend of a friend of a friend who overheard one of Saddam Hussein's body guards). These cables also provide knowledge on a source's motivation for providing the information, his or her track record, as well as the results of any background investigation done on the source. Sometimes it is information deemed too sensitive to even put in an intelligence report. Sometimes it is information that the report writer does not realize is significant so it is left out even though, combined with other information, it would help put pieces of the puzzle together. The decision of what goes into a CIA report *vice* what remains unpublished is primarily left to the discretion of the CIA station chief. The power that this individual has to protect sources and methods is often to the detriment of all source analysis used to make connections. Insiders refer to the intelligence value in these ops cables as "intelligence masquerading as operational data." No analyst who has had access will sincerely argue that there is not tremendous intelligence data in these cables. The argument against access to them is that there is also operational data that analysts do not need and should not have. Reforms over the years to try to do a better job of separating the intelligence from the ops cables, however, have failed. The only process that has worked, to date, is to give analysts access to the cables themselves. Yet, the CIA/DO has resisted this and will continue to resist to a degree that is almost inexplicable. This report will explore the reasons why later on.

FISA Information

The Foreign Intelligence Surveillance Act (FISA), passed in 1978, provides a statutory framework for the use of electronic surveillance to gather foreign intelligence. Currently based on the guidelines of the FISA Panel, four of the national CT centers have direct access to intelligence obtained through these court orders: CIA, NSA, FBI, and NCTC. Some of the FISA intelligence does make it into reports, but the data that goes unreported is vast. Senior analysts interviewed expressed much concern that the agencies with direct access to FISA-obtained data were not doing near enough to get the valuable intelligence out to the other national CT centers.

CIA/FBI Communications on Ongoing Terrorism Investigations

These communications range from FBI updates on status and/or new developments, to specific queries from the CIA on information or action they want from the FBI. Other than NCTC, national CT centers are not privy to the communications between the CIA and FBI concerning on-going counterterrorism investigations. Analysts outside the CIA or FBI assigned to the NCTC are amazed when reading these cables and are invariably left with the impression that the CIA and FBI still believe they are the only ones trying to stop terrorists attacks.

Direct Translation of NSA Intercepts

NSA intelligence cables are often based on a multitude of different intercepts that linguists have translated. CT analysts have neither the desire nor the time to read all the translations – that is what the NSA reports officers are assigned to do. Nevertheless, there are times in the course of assessing and analyzing data that analysts require direct access to the translation. They may want access based on their instincts developed through years of intelligence work, or based on new evidence that has come to light. National CT analysts need to have equal access to these translations in all other undisseminated CT data. The next chapter explains why.

The Case For Equal Access

Common sense dictates that the U.S. government must fix this problem between the "haves and have-nots" of data access. Those with access cannot continue to believe they are the only players in the game. Why? Because this is neither a game nor a battle over turf; it is a race to save lives before terrorist attacks occur. While this author interviewed over forty officials, the 9/11 Commission and the WMD Commission interviewed hundreds and the message to all was the same: you cannot have analysts who are working the same problem operating with different sets of data – they need the same data. This chapter will discuss the premium on quality that comes with equal access, and the fact that the data is not an end in itself. Further, this chapter will discuss the need for a true IC enterprise that optimizes all its resources and analytical firepower to stop terrorist attacks.

Premium on Quality Data

Both camps, meaning those who are for and against greater intelligence sharing, generally agree that intelligence is a qualitative rather than a quantitative business. Yet, they fundamentally disagree over

what this means operationally. The collectors who control the data argue that, due to the massive amounts of data collected, it is incumbent upon them to sort through it to determine what is pertinent and credible and then report it to the other agencies. Although this argument sounds logical, it does not correspond to reality. In today's environment, there is a greater chance that agencies will report all information to prevent being accused of not publishing if an attack occurs, rather than reporting only what they deem credible. This is not a complaint. Most of the best analysts want to be able to skim through as much as possible and then zero in on what they deem important. As these analysts use all available sources of information they are often able to make connections between one set of data and another, which can turn seemingly non-credible information into vital intelligence. But right now, too many CT analysts waste time calling reports officers to ascertain relevance and are still often left wondering what is the real story as far as the actual raw data the report is based on. The point here is that national CT analysts do not have the ability to link to the unreported data so that they can perform their primary functions: analyze and assess. The collectors are right about the huge amounts of data that need to be sorted through. This is all the more reason why the U.S. government should utilize all the manpower in its national CT centers which will give it the collaboration and alternative analysis needed to most completely connect the dots.

The qualitative premium on unreported data is clearly evidenced by the IC culture that spends so much effort bartering for it. The success of an analyst is often based on his or her ability to establish interagency contacts (in order to get access to undisseminated data) rather than their ability to analyze. This is the culture that has evolved. Rather than actually collaborating with community analysts, they are really networking to see if the unreported data their contact is privy to is consistent with the analysis they have done with the reported data. They listen attentively while their contact picks at an aspect of their analysis based on undisseminated intelligence their contact has that they do not. They learn a seemingly good source is not so good after all or vice versa. They ask about the source line and are told to forget how the report describes the quality of the source. They trust their contact from experience, realizing the person cannot tell them everything but does always get them on the right track. These Woodward-Deep Throat-type relationships, which are prevalent around the community, need to be replaced with true collaborating relationships where both sides have access to the same data. The U.S. government cannot afford to have analysts with clearances acting like investigative reporters going after what is already known. There is no time for such an unproductive system and there has not been for quite a while. If the national CT centers were approved for access, the productivity of all CT analysts would increase dramatically as the need to spend time bartering would end and the focus would be where it rightfully belongs: analyzing data. Nowhere has this been made more clear than in a retrospective look at the IC analysis leading up to the 9/11 attacks.

Data is Not an End in Itself: The 9/11 Example

All too often, the collecting agency views the data collected as an end in itself rather than as information that requires all source analysis to help uncover terrorists plots. Yet, in the process of withholding sensitive data, there unavoidably is non-sensitive data within it that would have value if it were properly analyzed. It was this kind of non-sensitive data, embedded within the sensitive data and therefore not accessed, that was a lost opportunity in stopping the 9/11 attacks. Analysts do

not have time to read all the unreported data that is available, but the good ones have a knack of knowing when to link back to the raw intelligence as they sense it is warranted. This is how good analysts put the pieces of the puzzle together and is why the national CT centers need equal access: to ensure more talented analysts can come at the data from different angles. Different angles are what the IICT analysts bring to the process, and they do not care about where a CIA officer is going to meet a source (the sensitive ops info in these ops cables). They do, however, care about the "intelligence masquerading as ops data" that they need to properly do their job. It is this data that is so critical. One perfect example is the known but unreported information prior to 9/11 concerning two known terrorists, Khalid al Mihdar and Nawaf al Hazmi.

In January 2000, the CIA's Counter Terrorism Center (CTC) learned that Khalid al Mihdar had applied for a U.S. visa. In March 2000, CTC learned that on the 15th of January one of his associates, Nawaf al Hazmi, had flown to Los Angeles, California. This information was in unreported ops cables and not shared. There was no attempt by the CTC to find either individual.[4] In January 2001, an FBI agent investigating the attack on the USS Cole was able to determine a man named Khallad was involved with the attack and then the CTC ascertained that Khallad was an associate of Khalid al Mihdhar. The CIA did not let the FBI (or any of the national CT centers) know of this association and made no effort to find him or Hazmi in the United States. The 9/11 Commission reported, "this incident is an example of how day to day gaps in information sharing can emerge even when there is mutual goodwill." They went on to explain, "the FBI agent on the scene received copies of the reports that CIA disseminated to other agencies regarding the interviews. But he was not given access to CIA's internal operational reports, which contained more detail. It was there – in reporting to which the FBI investigators did not have access – that information regarding the January 2001 identification of Khallad appeared."[5] If all national CT analysts had automatic access to these ops cables, the "day to day gaps in information sharing" would be eliminated.

In fact, Midhar had accompanied Hamzi to Los Angeles on that January 15th flight. Then, in June 2001, Midhar left the United States and returned again on July 4th. FBI witnesses to the 9/11 Commission offered that even if Mihdar had been found there is nothing that they could have done except follow him onto the plane. The 9/11 Commission, however, argued that both Mihdhar and Hamzi could have been held on immigration violations or as material witnesses in the Cole bombing investigation and that other investigations and/or interrogations could have uncovered information leading to the attack or the other attackers. Yet, the main concern of the 9/11 Commission and others is directed at the lack of sharing between FBI and CIA. The question should not be what the FBI would have done, but what the community as a whole could have done if they had access. In this case, DIA would have jumped on this data due to Midhar's connection to one of the USS Cole attack bombing conspirators. DIA would have ensured the Naval Criminal Investigative Service (NCIS) (the U.S. Navy agency investigating the Cole attack) was aware. The NCIS would have easily tracked them down as they were using their real names living in San Diego, which happens to be one

[4] This is not meant to be critical of the CIA. If one knew the amount of data that comes across their desks everyday one would understand how this easily dropped through the crack. Equal access among the seven national CT centers will go a long way to fill these kinds of voids and ensure connections are made with the data the U.S. government has collected.

[5] 9/11 Report, chapters 5 through 8, direct quotes from 383 and 384.

of the largest concentrations of U.S. naval assets in the world. This fact no doubt would have alarmed the NCIS investigators even more. Why? Because of their roles and missions, they would have been focusing on the connection to the Cole bombing and what the two individuals might be planning in the United States. Would events then have led to an uncovering of the 9/11 plot? We will never know. The better question is whether we will have to ask a similar question again.

There is at least one FBI analyst who understands this. She was digging into the connections between Khallad (Cole bombing involvement) and Khalid al Midhar but was hindered, not by lack of data, but by lack of access to that data. The 9/11 Commission Report explains, "Because the CIA had not disseminated reports on the tracking of Mihdar, "Jane" did not pull up any information about Mihdar's U.S. visa or about travel to the United States by Hazmi or Mihdar."[6] It was not until August 21, 2001 – a mere three weeks prior to the 9/11 attacks – that another FBI analyst who was assigned to CIA's CTC (with access to unreported data) made the connections that led to Mihdhar and Hazmi being put on the TIPOFF watch list. These connections were made after an FBI agent, who lacked access, requested their representative in the CTC review all the unreported data again. The data used to make the connections had been available at CTC for a year and a half. This information was not sensitive operational data but rather a perfect example of vital "intelligence masquerading as ops data."

This author was able to review ops cable traffic related to 9/11 after the fact and was astounded by the amount of undisseminated data available only to CTC. Another example released through the 9/11 Commission Report is the now famous "Bin Laden Determined to Strike in U.S." memo prepared for President Bush. One would think the entire CT community would have had access to this report or the data in it. Yet, the 9/11 Commission Report indicates that, when it was published for the rest of the community the following day, it "...did not contain the reference to hijackings, the alert in New York, the alleged casing of buildings in New York, the threat phoned in to the embassy, or the fact that the FBI had approximately 70 on-going bin Laden-related investigations."[7] Although in the aftermath of 9/11, the NCTC was approved to release the Presidential brief to senior members of the national counter terrorism community, it did not last long. As soon as there were a couple of examples of people in giving access to individuals who were not specifically cleared for it, the information in the President's daily brief was taken away from the national counter terrorism centers outside the NCTC and CIA. Instead of coming down hard on those who broke the rules, the incidents were used as the excuse needed to once again restrict access.

There are many more examples of data access issues in the 9/11 Commission Report including connections that could have been made between now-convicted 9/11 conspirator Zarcarias Moussaoui, Khalid Sheikh Mohammed (mastermind of the 9/11 attacks), and al Qaida. Multiple groups, such as the Markle Foundation, have even determined retrospectively that if all known data (public and private) had been accessed and assessed, all 19 hijackers could have been uncovered prior to the events of 9/11.[8] A post 9/11 review clearly shows that data is not an end itself, but

[6] Ibid., 386.

[7] Ibid., 377. This author knows as a matter of personal experience from June 2003-2005 and through interviews through May 2006 that this procedure of taking out the good tidbits of unreported information from the Presidential briefs before sending them out to the rest of the community is still the norm today.

there is also the point that direct access is required even when data is not intentionally withheld but has been tarnished by natural human ambiguity.

Human Ambiguity

Although much data is purposely withheld because it is deemed too sensitive, there is also concern that national CT analysts do not always receive the full meaning of the data even when there is no intention to withhold information. When CT analysts are limited to only what a reports officer (RO) has written instead of being able to link to the source of the report, he or she then has to contend with the ambiguities created by the RO's interpretation of the data. Anyone who has been in a classroom where the teacher whispered a statement to one student who then passed it along to the next knows that the last student invariably is told something quite different from the teacher's original information. This simple example illustrates how ambiguities can innocently set in when an intelligence officer writes a report based on intelligence given to him. What is needed to offset this natural ambiguity is ubiquitous collaboration so thoroughly ingrained in the IC business process that sharing it is no longer a conscious act. Only then will we optimize our resources as an intelligence community.

Optimize Resources and Productivity with a True Intelligence Enterprise

The 9/11 Commission Report stated that the head of the FBI counterterrorism unit, "felt deeply something was going to happen. But he told us the threat information was 'nebulous.' He wished he had known more. He wished he had had 500 analysts looking at Usama Bin Laden threat information instead of two."[9] Following 9/11, all the national CT centers grew exponentially. The CTC and DOD's CT agency (JITF-CT) both more than quadrupled in size. NSA numbers continue to grow rapidly, adding approximately 11,000 additional billets in the next few years. New agencies, such as DHS and NCTC, are growing rapidly. The FBI and the other national CT centers now have the numbers they need but are still faced with one major problem: they still do not have access to unreported data. Conversations with analysts just completing a rotation in NCTC and returning to their home agencies reveals that little has changed regarding access to unreported data for the other national CT centers. Requests from agency representatives inside the NCTC to pass along pertinent information to their home agency analysts are repeatedly denied. Even if they were not denied, this would only give them information someone has already determined is important rather then equal access to all the relevant data, which would enable more analysts to discover what the data is trying to communicate. Institutionalizing an automatic data access process is key. One would think that in light of the direct evidence laid out in the 9/11 Report, that in addition to an increase number of analysts, the CT centers would also have obtained increased access which is desperately needed for better CT community teaming. Instead, the bureaucratic tendency to throw money and resources at the problem without really focusing on efficiencies and effectiveness has so far prevented them from achieving the desired result.

---

[8] Markle Foundation Task Force on National Security in the Information Age, *Protecting America's Freedom in the Information Age* (October 2002), 28.

[9] 9/11 Report, 380-381.

Along with resources, what is sorely needed is the tremendous benefits of teaming between intelligence agencies. Congress achieved the needed teaming of the military services with the Goldwater-Nichols Act. The Executive Branch, Congress, and the DNI must now do what is required to get this same teaming throughout the intelligence community. In the military, when a soldier performs a joint assignment outside his service, it is viewed as a temporary shortfall that ultimately pays great dividends to the home service. When personnel complete joint tours of duty or tours in the other services, they return to their home service with a wealth of experience and insights which are immediately put to use. Although some may argue about the optimal number of joint tours that are appropriate, there is little argument about their necessity, nor about the fact that it was the Goldwater-Nichols Act that moved the military to the integration sorely needed to fight wars. Congress made it possible with very detailed and complex language, and gave it teeth through strong oversight.

Unfortunately, Congress has not even come close to achieving this same integration for the IC. Although IC members do have various IC career broadening programs and liaison positions, officers returning to home base find that their new expertise is not utilized in the work place and that they are not rewarded with career-enhancing opportunities. The NCTC is a perfect example, as it has a multitude of intelligence officers on loan from other national CT centers who then rotate back to their home agency. Although the analysts do return more seasoned and experienced, they also return without the access they enjoyed while at NCTC, with disastrous consequences. The knowledge they bring home is the breadth and scope of intelligence data that their home agency is left out of. The one common factor of almost all returnees is the extreme frustration of having to continue to try to connect dots, knowing full well that there is a significant amount of unreported data that would help them contribute if they had access. Their frustration spreads and impacts the overall morale of their agency. Instead of a positive dividend, the home agency is left with leadership challenges to retain quality personnel. One veteran impressed upon me the standard quote he gives to all these type of rotational returnees, "analyze the information you have, not the information you wish you had." A sad but true answer, unfortunately.

Returning analysts, therefore, fall into three main categories: those who change agencies to gain access, those who quit altogether, or those who stay and keep their frustration bundled up. This scenario is repeated over and over again throughout the national CT centers. These are not just leadership challenges but national security voids as the federal government is not properly utilizing the unique resources it has at its disposal to fight the war against terrorism. No matter what teaming initiatives might be put into place, they will all fail if equal access to data is not part of the equation. Where this is most notable is the lack of analytical optimization of the best and the brightest CT community analysts.

Senior Analytical Talent is Wasted in CT Agencies that Lack Access

As post 9/11 CT center billets grew, so did the demand for experienced analysts. This demand resulted in each agency recruiting senior talent away from each other with the brand new DHS leading the way. In normal circumstances, spreading the wealth is a good thing, but not when talent is wasted in agencies that lack access. The IC spends years grooming some extremely talented CT analysts who have a knack for picking out pertinent reports, linking them back to the original

intelligence when warranted, and then making connections. Not only do these analysts have a "need to know," the United States and its people have a need for them to know. One may therefore ask, what do these star analysts do instead? Some continue to nurture relationships of trust in the bartering system previously described. But, however adept an analyst may be at the bartering game, it still only gains him or her access to what is already known, not the connections that remained unconnected because they were not given the opportunity to uncover them. It is critical that the relationships these analysts develop be used for proper collaboration rather than unproductive attempts to gain access, which also bring the risks of security leaks due to the fact that they are not read into the sensitivity of the data. The U.S. government cannot afford to have situations like the months prior to 9/11 where only a small number of analysts had the access that was required to ascertain that two terrorists had arrived in the United States. Yet, these scenarios continue. One specific example given to this author involved a small team of CIA analysts who were tracking one of the post-9/11 threats that had unnecessarily distracted our government. A member of this small group admitted to a senior DIA analyst that they would have been able to discount the threat much sooner if senior talent from the rest of the community had been "read-in" and collaborated with them. If this is not fixed, we will lose this talent and lose any advantage gained by individuals rotating through the NCTC. One may ask, if it is so obvious that equal access is required, why are we not there yet?

The Obstacles, or Why is it So Hard to Get There?

As the United States heads into its fifth year since the attacks of September 11th, it is not near a solution that would optimize the analytical firepower and unique perspectives of all the national CT centers. Why not? We can safely say that it has not been due to a lack of attention, as illustrated by the recommendations made by the 9/11 and WMD Commissions and the mandates written in the IRTPA. This chapter will explore the bureaucratic tendencies in the IC to protect one's turf that feed the culture to over-compartmentalize information. Then it will look at a recent attempt to bring about better sharing in the NSA and the evolution of intel sharing within the CIA. This chapter will explain how intelligence collectors, those still in charge of "need to know," have failed to understand or accept the value-added of all-source analysis. The collectors of data are accustomed to the clamoring for access that occurs when a terrorist event takes place and they were well prepared for the post-9/11 battle to attempt to take control of the data their agency collects. Decision makers need to understand this tendency to tighten controls when the demand for access increases so that they can force change by handle security concerns in ways that do not restrict access to those at the forefront of connecting the dots.

Bureaucratic Protectiveness and Prejudices

In several interviews conducted for this paper, officials were asked what they believed to be the number one reason why data access is so hard to achieve. The answer was almost always the same: "information is power." Even though the NCTC made historic progress by gaining access for its agency, it is not achieving data access for other agencies as mandated by the IRTPA. Could one reason be that if all CT centers had the same access as NCTC, NCTC's value would drop, at least according to this "information is power" argument? Is this not the same reason why it was such a struggle for CIA/DI analysts to get access to CIA/DO ops cables and NCTC to get this same access?

Even if the NCTC somehow rose beyond the bureaucratic tendency not to share and tried to grant access as the IRTPA mandates it to do, it would not be able to do it. In order for the NCTC to achieve access for itself, it had to agree to get permission from the collectors before passing along undisseminated data to someone else. To these requests the collectors invariably answer no. Why do the collectors invariably say "no" to the analysts but at times allow senior officials in on the most sensitive of data? Whether collecting agencies admit it or even recognize it, the main reason information is kept from analysts working outside the collecting agency is to ensure the agency's position in the fight for mission and money. Members of these agencies argue, and most often sincerely believe, that information is held for national security reasons, when in reality they are jeopardizing U.S. national security much more by denying CT analysts the data they need to carry out their basic mission of "connecting the dots." They do not recognize, and the U.S. government should not depend on them to recognize, the tremendous value the other national CT centers bring to the fight.

This same bureaucratic protectiveness contributes to misunderstandings about other agencies. The most common misunderstanding is that other agencies cannot handle all the collected data in a qualitative way. Rather, so they say, it is the collecting agency's job to evaluate it and deliver it to the consumer so their customers do not bury themselves in extraneous details. This explanation is credible in instances where getting intel to the law enforcement community is critical in enabling them to properly focus their security measures and warn citizenry. But this view is completely wrong when referring to fellow CT analysts who are highly qualified and paid to analyze terrorism data. Despite the lessons of 9/11, collecting agencies have not been swayed against their conviction that analysts are just folks writing summary reports and presidential briefs based on data others collected with no real value added. This misunderstanding is exemplified by one of their most common questions to those who want access. They ask, "since you cannot use unreported data in the production of your intelligence reports, what good does it do for you to have access to it?" This attitude completely misses the point that CT centers need the data to strengthen their ability to make connections. When connections are made the normal approving authorities will sometimes then see an obvious need to further distribute the information to protect against the threat with all the normal operational considerations taken into account. Since the problem stems largely from perception reinforced by institutionalized prejudice, only strong leadership will overcome this most difficult bureaucratic hurdle.

Difficulties in Gaining Access to NSA Data

The NSA has strenuously resisted giving their direct translation of intercepts to anyone outside of the NSA, including even their sister DOD agency, DIA. Yet, Executive Order 12333 (United States Intelligence Capabilities) designated the Secretary of Defense (SecDef) the executive agent for the United States government's signal intelligence communication security activities. In turn, the SecDef delegates this responsibility to the Director of the NSA (DIRNSA). One would think that with this line of authority it would be easy to get the NSA to share their terrorism data with fellow DoD CT analysts. So thought Lieutenant General Keith Alexander when he took the reins of NSA in August 2005. Yet, according to a senior Senate staffer, his ideas of raw data collaboration across agencies to work problem sets are meeting with tough resistance. The NSA lawyers sincerely feel they cannot share NSA raw intelligence with anyone outside the agency because of a classified DoD

directive that has EO 12333 implementation guidance written by the Attorney General's office that they believe prohibits them from doing so. More than four years after 9/11, the rules that NSA lawyers believe they are operating under have not changed. They believe the NSA is assigned under EO 12333 exclusive roles and responsibilities for protection of privacy of U.S. persons. The NSA trains its employees in handling information about U.S. persons (known as minimization procedures), it has electronic audits set up to monitor and ensure its analysts are complying with the minimization requirements, and the DIRNSA has authority over to discipline employees if they violate those rules and procedures. The NSA lawyers exert that allowing outside analysts access to this data without having first gone through NSA training while not being subject to NSA auditing and disciplinary procedures is prohibited. One has to wonder how much of the bureaucratic tendency of holding back this information is due to the "information is power" argument rather then trying to follow Attorney General guidelines. If those guidelines are the problem, why is NSA not asking them to be reviewed or EO 12333 to be rewritten so the guidance can be modified if necessary? As this example illustrates, even a three-star general in charge of the agency, with a vision for data access and collaboration across agencies, is having trouble executing it. If General Alexander is frustrated in implementing his data access vision even within DoD, one can then start to understand how much harder it is going to be to force the CIA to share its own unreported data.

Unfinished Business: Gaining Access to CIA Ops Cables

In the CIA, the collectors are in the Directorate of Operations (DO) and the analysts are in the Directorate of Intelligence (DI). The DO and DI have historically been at odds when it comes to the DI analysts gaining access to CIA ops cable traffic. The Director of Intelligence himself receives his access like many others in the barter system: establishing and maintaining the personal trust of his compatriots in the DO *vice* an automatic access based on what should be his "need to know." In 1987, the CIA made a fundamental change to who gets access to its ops cables within the agency. For the first time, DI analysts assigned to the newly formed Counter Terrorism Center (CTC) were given access to the ops cable traffic related to terrorism. The CTC was formed to integrate the counterterrorism portions of the operations directorate with the analysis directorate. The CTC became a major success story. Not only did analysts benefit from the arrangement, but the collectors did too. Better access led to better analysis, and analysts in turn were able to ask for more specific collection, which ultimately improved their assessments and their ability to connect data streams. Strong criticism did exist, however, that the improvement did nothing to help other national CT centers. Following the events of 9/11, the IRTPA attempted to address this issue by the creation of the NCTC. Predictably, the same office that resisted the creation of CTC, CIA/DO, also resisted the creation of the NCTC. Once created, the DO then heavily resisted giving NCTC access to its ops traffic. Ironically, they used the existence of CTC, which they initially did not support, to argue that NCTC was not necessary.

The inroads made by the first NCTC Director, John Brennan, have been nothing short of historic. As a result of his efforts, for the first time the CIA allowed someone outside the CIA to have access to their unreported information. He also brought representatives in from other agencies, including representatives from all the national CT centers, and gave them unprecedented access to this information. Unfortunately, however, this increased access was accompanied by a strongly enforced policy that the information could not be released to their home agency. The next key step in this

forced evolution will be for the rest of the national CT centers to have the same access NCTC has been able to achieve thus far. It should be pointed out that only a few of the officials interviewed were optimistic that this will ever happen, and even they felt another 9/11 type event will have to occur first. Later on this paper will offer a path on how to get there, with the number-one recommendation addressing why collectors can no longer be allowed to define "need to know."

Data Collectors Should No Longer Be Allowed to Define "Need to Know"

During the course of several interviews conducted for this paper, some clear lines were drawn between those who believe in a very strict "need to know" and those who believe in a "need to share." The 9/11 Commission wrote that the "need to share" must replace "need to know" as if they are two diametrically opposed concepts. This is a dangerous way to word the argument because it gives fodder to those arguing that we are sacrificing security by sharing. The "need to know" concept is perfectly valid. *The problem is that, despite the lessons learned from 9/11, the U.S. government continues to allow the collectors of data to define who has that "need to know."* It is naïve to expect a collecting agency to spend time assessing whether other agencies need its data. As long as the collectors control who gets access to the data their agency has collected, they, in essence, are deciding that other CT centers are not equally capable and do not have the mission to connect the dots.

This directly contradicts the whole concept of the IICT warning community introduced at the beginning of this paper. CT centers that do not have access to unreported data are clearly not on equal footing when trying to do their part in the IICT warning process. A national level CT center may want to issue a warning due to the analysis of available information only to be told that it is neither necessary nor urgent based on information they are not privy to. There have been times when, instead of a community warning, the NCTC issues a private warning due to the fact they cannot get permission from the collecting agency to even coordinate the warning product. The fact is that national CT centers sometimes must bow to the NCTC IICT representative in the collaboration and coordination process solely based on information they are not privy to. Such a situation clearly undermines the notion that all CT centers are equal players.

Perhaps this point may be better illustrated with a real world example. The CIA has threat information related to DOD personnel in "Country X" that came from the interrogation of a high-level terrorist the CIA does not want anyone to know has been apprehended. Therefore, they choose to provide the data only to the NCTC with the restriction that no other national CT center may have access, including DoD's CT center (JITF-CT). A JITF-CT representative inside the NCTC is very concerned about this restriction and ultimately convinces the NCTC, which then convinces the CIA to hook up the CIA station chief in "Country X" with the local DoD commander to inform him of the threat so he can take appropriate force protection measures. The CIA rationalizes that the JITF-CT did not have the "need to know" but the local commander did, so their job is done. In their view, the "need to know" was reserved for those directly threatened (after some arm twisting). What is always missed in these types of scenarios is the possible connections other national CT centers may have made drawing on their different perspectives and their analysis of all the available information. Further, because they were not privy to the apprehension of the terrorist, they are not able to submit questions to the interrogators that may have garnered more information from the detainee. In

addition, they are not seeing the interrogation reports from this high-level detainee, which may have helped them make new connections. Instead, CT analysts waste resources trying to track down a terrorist that is already detained.

This type of event continues to happen frequently, despite the lessons learned from 9/11. Why? As already stated, the collector is deciding "need to know." *The DNI must create an independent body to make "need to know" determination, which is, in fact, a crucial part of a slow revolution that has been percolating for years.*

The Collectors' Arguments Against Granting Access: Damage of Unauthorized Disclosures

The main legitimate reason for limiting access is due to the harm of unauthorized disclosures. No one articulates the concern more ferociously than retired CIA Director R. James Woolsey. In testifying to Congress, he explained that he believes the 9/11 Commission has some good ideas but they tilted too far when it comes to sharing information.

> *"sharing is fine if you're not sharing with the Walkers, Aldrich Ames, Robert Hanssen, or some idiot who just enjoys talking to the press about how we are intercepting bin Laden's satellite telephone calls. Hostile infiltration into our government, or for that matter blabbermouths, are not solely "Cold War assumptions" that are "no longer appropriate" as the Commission suggests. Before it adopts the Commission's view that sharing should generally trump security it might want to look carefully at Wahhabi/Islamist infiltration into our prison chaplains and perhaps other parts of our government – in my view, such infiltration should be treated seriously, and may be a larger, not a smaller, problem than during the Cold War."*[10]

This argument about the harm of unauthorized disclosures can be broken down into many pieces. This chapter will try to address them all in turn.

Foreign Countries Will Not Share If We Share More Broadly

Our allies and coalition partners are concerned about our leaks and will not share with us if we share more broadly within the intelligence community, or so the argument goes. This argument is weak when it comes to sharing with the national CT analysts. In fact, this author became privy to several cases where the CIA had threat information related to DoD but would not release it based on these agreements. One case involved specific DoD related threat information that came from one of the U.S.'s strongest allies. Anyone familiar with the exceptional ties among the intelligence agencies of the U.S. and this unnamed country would know that officials from this country would be appalled if they knew this DoD threat information had not been passed to DoD terrorism analysts. They would be even more appalled to learn they were used as the excuse for not sharing it.

It is true that the U.S. government has information exchange agreements with nations that share with the United States. It is also true that the same people who negotiate these agreements are the

[10] Testimony of R. James Woolsey to the U.S. Senate Committee on Governmental Affairs, *Hearing on the 9/11 Commission's Recommendation,* August 16, 2004.

collectors of data who want to keep the information within their agency. With that in mind, it is easy to ascertain why the agreement might say, for instance, the information shared with the United States must remain within "CIA channels only." The DNI can easily take steps, to be laid out in a later chapter, that will increase confidence of our foreign government sources that their intelligence is safe with the United States. Affected agreements will need to be renegotiated by unbiased negotiators from the DNI with the understanding that the intelligence will be shared with the appropriate national CT centers under a new system that is tough on inappropriate disclosures. This is where our focus should be rather than keeping data from CT analysts who truly have a "need to know."

Loss of Source Recruitment Due to Unauthorized Disclosure

Another weak argument is that we will lose our source recruitment if we begin to share data within the CT community. Just as with foreign governments, if we show we are serious about stopping leaks, we can increase the confidence of sources to levels not yet seen. There is no reason to assume that disclosures will rise with better access to national CT analysts, just as there is no evidence that this occurred when the two biggest collectors, NSA and CIA, hired more analysts. Increasing numbers of analysts with access does not seem to matter to the collecting agency when they are analysts within their own agency rather than other intelligence agencies. That is the whole point; all intelligence personnel must be viewed as the same employees - the DNI must take control by standardizing security practices throughout the community. When there are leaks despite the best efforts to prevent them, the DNI must investigate and punish. Source handlers will handle their recruitment issues as they always have: increased compensation packages to the sources, relocation of family, health benefits, whatever incentives it takes. Yet, this will not be done due to increasing access to analysts but rather because of political leaks that have always plagued the community.

Not All CT Centers Are Created Equal/NCTC Solves the Problem

Some argue that the national CT centers are not created equal due to the concern of unauthorized disclosures. The most sensitive information needs to be kept centralized so that it is protected by direct control of the personnel who access it, with tight security and counter intelligence (CI) safeguards to ensure its protection. If all the CT centers had the same access, you would not need an NCTC, or so the argument goes**.** This argument fails simply because NCTC cannot do it all and is not designed to. The IRTPA states the NCTC is to "ensure that agencies, as appropriate, have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analysis." Further, it states that the NCTC will "ensure that such agencies have access to and receive intelligence needed to accomplish their assigned activities." The IRTPA also states that the DNI, "shall, to the extent appropriate and practicable, ensure that each national intelligence center under subsection (a) and other elements of the intelligence community share information in order to facilitate the mission of such center."[11] Leaving the connecting of the dots solely on the shoulders of the NCTC is a grave miscarriage of U.S. government capabilities. The connecting of dots is just too difficult to expect one organization to do; the events of 9/11 proved the importance of ensuring the U.S. government is utilizing the perspectives of all the national CT

[11] Intelligence Reform and Terrorism Prevention Act of 2004, Subtitle B, Sec 1011.

centers. The collectors do have a right to be concerned that other agencies do not follow their same security safeguards. To address this valid concern, the DNI must standardize community security procedures and CI safeguards. Once they are standard, the NCTC certainly should use its leadership role to ensure teaming with all the national CT centers. This author believes the Directors of each national CT center would gladly give the NCTC federated tasking authority over them in exchange for equal access to information.[12] Only equal access will ensure the optimization of the tremendous cumulative capability of the national CT community. Those who argue for a solely centralized analytical capability are in the same group that argued against the creation of the CTC and the creation of the NCTC. This group controls access now within their agencies. The U.S. government must ensure that this power is taken from them.

Where Do You Draw the Line?

Certain collecting agencies also argue that if you start giving access to unreported data beyond the NCTC, where do you draw the line? If the CIA learned bin Laden's location, do all the terrorism analysts really need to know of the preparations to grab him? If leaked before the operation, according to this hypothetical situation, we would lose the opportunity to apprehend him. In actuality, there are stringent procedures and safeguards in affect that drive sensitive situations such as this by restricting the information to a small number of people. But even then, you have to ensure that the right people know. One could just as easily argue that a DIA analyst somewhere in the bowels of the agency could coincidently be studying the very location of the planned operation and know pertinent information valuable to operational planners. There must be a process to take advantage of these pockets of expertise. It should not just be seniors at CTC and NCTC that have access to this type of restricted information. For instance, if the seniors at JITF-CT were aware of the pending operation, they could request authority to bring that unknown analyst into the fold. Instead of asking where are we going to draw the line, the question must be who are we going to allow to draw the line. As previously stated, this authority must be taken from the collecting agency.

The Harm of the Disclosure Itself

There is no question that unauthorized disclosures do serious harm to our national security and sometimes cost lives. To argue otherwise would be irresponsible. Yet, to state that the solution to this problem is not to grant equal access to all national CT centers is missing the point. CT analysts need access to all the relevant information available to perform their core function of making the right connections and discerning meaningful patterns. Unauthorized disclosures need to be dealt with as this paper will argue later. The focus needs to be against leaks from senior officials coupled with mammoth high tech counterintelligence (CI) safeguards that need to be designed to protect the Information Sharing Environment that the ODNI is in the process of creating. But it needs to be clearly understood that this is a separate issue from making valid "need to know" determinations. Unauthorized disclosures should never be used as a reason to limit access to raw terrorism data required by all national CT centers in order to stop terrorist attacks.

[12] In one interview, for example, this very question was posed to the director of a national CT center, and the answer was a resounding yes.

Legitimate Argument for Protecting Unreported Data Becomes Illegitimate When Applied to Analysts Working the Same Problem Set

The threat of leaks and unauthorized disclosures is very real and must be guarded against. But who is leaking this information? This chapter will argue that most leaks come from government officials with a political agenda, not from analysts. When leaks are made by analysts they are usually inadvertent and making better "need to know" determinations will actually help ensure the right people are read in to the program which in-turn will help decrease these types of leaks. *The U.S. government needs to ensure that analysis does not suffer in the process of trying to protect information.*

The intelligence most often leaked is that which is deemed too sensitive for the analysts. It is information given directly from a collecting agency to high-ranking officials with guidance that they cannot share with anyone else. But, as one senior official admitted in a recent interview, this official then tells his or her significant staff and gives them the same guidance not to tell anyone. This continues down the chain of command and somewhere along the way someone leaks the information while the analysts who truly had the "need to know" never even knew the information until they read it in the newspapers. Senior officials interviewed from administrations spanning Ronald Reagan through George W. Bush expressed surprise when they were told the raw data they could ask for and receive was not available to all of the national CT centers. It is essential for decision makers to realize that we have a multitude of qualified analysts that do not have access to unreported information under the misguided logic that it is too sensitive even for those trying to stop terrorist attacks. Time after time, insiders will tell you that it is not the number of personnel who have access that correlates to leaks but rather who it is exactly that has access. Limiting access did not stop the recently revealed NSA program from being leaked even though only eight senior individuals where aware of its existence and the analysts assessing the data were not even aware of how it was gathered. Analysts, it is safe to say, rarely are the problem when it comes to leaks. The problem is making sure the right people get told, with proper guidance.

In Order to Keep a Secret You Must Tell the Right People

Although this statement seemingly contradicts itself, understanding it is important in order to start changing the culture of the IC to enable better sharing. Perhaps the best way to illustrate this point is through two real-world scenarios.

In the first scenario, an intelligence officer who works on a 24/7 watch is charged with validating requests for imagery collection. His job is to ensure imagery requests meet certain criteria that justify their requested priority to ensure that the limited imagery time is spent acquiring the pictures that are most important. The officer begins to notice some of the requests had justifications that did not quite make sense and so he begins to turn down or lessen their priority in order to ensure that they do not stop higher priority requirements from being collected. One day the officer is called into his boss's office and told to stop questioning and talking about these "bogus" requests for imagery and just process them at their requested priority. He is told their true nature was classified in a special compartment that he was not authorized to know about. It is further explained that his questions were putting the entire program at risk of being disclosed, so he needs to cease and desist. The officer instead suggests that he be read into the program so that he then knows when one of

these requests is being processed and therefore would not question it. He is told that is not possible. He then asks his boss, how is he supposed to do his job? Is he supposed to just assume every request that doesn't meet the established criteria is from this highly classified program? After much argument, the officer is read into the program. Once "read in" he immediately understands the need for secrecy but he also understands the need for others doing his same job to be read in. So he asks that his colleagues be read-in but his request is refused because there is a quota on how many people can be read into the program. Over time, others who have that officer's job raise the same questions and finally, after two years of dealing with these questions, approval is granted to read them all in as it becomes obvious that it is needed to protect the program. In other words, telling more people (the right people) stopped the asking of questions, which ultimately helped keep the program secret.

The second scenario involves an officer who runs a DoD counter terrorism office in the Pentagon. This officer briefs a two-star general every morning before the brief is taken to the Chairmen of the Joint Chiefs of Staff. One morning, the officer arrives at 4 am to find that word has leaked to some of the CT 24/7 watches that something big in the CT world happened overnight, but no one knows what it was. This starts a rush throughout the CT community to uncover the news. The officer, like many other senior CT officers, begins phoning around the community, trying to learn the news prior to the morning brief. The more calls that are made, the more people learn that something big is up. One of the calls this officer places is to a JITF-CT liaison officer overseas, who is asked if he is aware of a big arrest or some other big event that may have happened. After much pressing, the liaison confides that indeed a key terrorist has been apprehended. When the officer briefs the two-star behind closed doors, it is obvious that he already knows, and the two-star instructs the officer not to tell anyone as this affects current operations. The officer tells no one, but the quest for the information is so strong that, by the end of the day, almost the entire IC is aware of this high-level arrest. Reliable sources eventually indicate to the officer that, when this all kicked off, the new DNI had instructed that only seven high-level government officials be briefed on the news and no one else. By trying to keep this information too secret, everyone found out.

One may by now wonder the relevance of these two seemingly hypothetical scenarios, but they did in fact take place, and were experienced first-hand by this author. These are by no means rare events; they happen every day in the IC. Often word gets around due to personal relationships and the fact that members of the CT community who do have direct access recognize their compatriots in the other CT centers do have a "need to know." They can now justify their actions by the fact the President, through EO 13388 (Further Strengthening the Sharing of Terrorism Information to Protect Americans), and the Congress through the IRTPA, direct them to share. Once they confide in someone who does not have direct access, it is a little easier for that person to confide in other analysts because they do not fall under the same security rules as those who have direct access. When analysts are forced to barter for the information they need to do their job, there is a risk they may uncover compartmented information without realizing its operational sensitivity because they have not been read into the program. Yet, if the "need to know" is properly defined, so that the right people are given access in the first place, the need for the bartering system to ascertain unreported data is greatly reduced. Established relationships then are used for critical collaboration on an equal level. In addition, there is no longer a contradiction between agency policy and existing

law. It then becomes much easier to bring stiff penalties to anyone who breaks agency policy, as the excuse that analysts have to let others know has been eliminated.

If you tell the right people and have strict standardized security and counter intelligence (CI) practices, the risk of disclosures goes down significantly while the productivity of analysts goes up exponentially. This is much easier said than done; the next chapter addresses a way to get there.

How Do We Get There?

There are so many voices crying out for intelligence reform and so many different stakeholders that decision makers are undoubtedly overwhelmed. John Brennan put it very well:

> *"Don't get me wrong. Reform is needed to mesh the human and technical capabilities now scattered through the government. But instead of prompting greater integration, the September 11, 2001 attacks and the controversy over inaccurate intelligence about weapons of mass destruction in Iraq unleashed a torrent of conflicting study commissions, statutes, executive orders, presidential directives and departmental initiatives. What's still missing is a coherent framework of reform. The rush of initiatives has resulted in no overall strategic plan."*[13]

As the DNI puts together a strategic plan, it is critical that "need to know" determinations be taken away from the collectors. Both the 9/11 Commission and the WMD Commission recognize this, but their recommendations have not gone far enough to make it a reality. The IRTPA at least gives the DNI the authority it needs, and it is now up to the DNI to take whatever actions are necessary to make it happen. There are two critical steps necessary to stop the collecting agencies from making the decisions on data access: data access identifiers and an arbitration authority. This chapter has many other recommendations, just as the commissions had, but they are all irrelevant without implementing the first two.

Data Access Identifiers that Define "Need to Know"

The DNI must create all powerful data access identifiers across agencies tied to an organization's DNI validated mission and ability to consume and analyze available data. This huge undertaking will need to encompass the roles and missions of all in the IC community. At a minimum, the final result should include the determination that national CT centers have the same data access as CT analysts working at CTC and NCTC. To be successful, the DNI will have to ensure everyone understands the seriousness of the new reforms. One way to do that is to call all the CIA Station Chiefs home along with seniors from other collecting agencies. The DNI or, even better, the President then seats them down and explains that this is the way forward and if anyone cannot accept it they need to resign. The DNI should be prepared to address their concerns but also be prepared to fire those who stand in the way. The firings need to be announced to the whole community so everyone knows the leadership is serious about reform.

[13] John Brennan, "Is this Intelligence? We added Players, but lost Control of the Ball," *Washington Post*, November 20, 2005.

Arbitration Authority

It is absolutely essential to have an independent arbitration mechanism established by the DNI. This higher authority must be composed of individuals free of bias who can weigh the concerns of the collecting agency with the concerns of an agency's appeal for access. This is a difficult but essential task, and the DNI must seek out talented leaders who have a reputation for fighting for equal access. This type of individual will be critical for the success of the arbitration authority.

After executing these essential first two steps, the ODNI must constantly get feedback and provide oversight to determine if real change is happening. If it is not, more drastic changes will be required such as the ODNI actually taking over the functions of reports officers at the collecting agencies so they can directly control dissemination of the agencies' collected intelligence.

There are many other actions that are necessary to create an environment where expanded access can succeed while decreasing unauthorized disclosures. The CIA has just recently cracked down on leakers within its agency, but what is needed is a standardized policy throughout all the intelligence community. Not only will this reduce disclosure risks, but it will create an environment of teaming that is focused on overcoming the culture that resists sharing while creating healthier competitive analysis.

IRTPA & Goldwater-Nichols-Style Standardization Security

Attaining proper intelligence teaming will take years, just as gaining jointness did among the military services, but the DNI needs to move now to set the stage for long-term success. Unfortunately, in comparison to the Goldwater-Nichols Act, the IRPTA falls short in transforming the IC into a joint team as several commentators have pointed out. This is easy to understand if you consider the fact that the Goldwater-Nichols Act was drafted over a four-year period and the legislators knew every line and why it was written. Once passed, they methodically and relentlessly enforced the Act. In comparison, the IRTPA was drafted in a few months and the committees that wrote it are not the same committees with oversight jurisdiction, making it much more difficult to enforce.

Yet, despite its flaws and the ambiguities, the IRTPA created the DNI and gave him the authority he needs to create an information sharing environment, to make sweeping changes, to standardize community security practices, and to hire and fire. The DNI, with the President's support, can put into place measures required to obtain equal access. These actions, at a minimum, need to include standard CI safeguards that include automated monitoring and auditing of data access, standard restrictions on use of the data, and timely investigations and enforcement of the rules. In addition, clear criminal, administrative and financial penalties need to be in place for those who attempt to circumvent access as well as monetary awards for those who fix data access issues. Standard policies for hiring, training, security, polygraphs, and nondisclosure agreements are required for those within the intelligence community. Further, there needs to be joint intelligence billets with assignments to them being necessary for promotion. One cannot become a general officer in the U.S. military without having done at least one joint assignment.[14] Lastly, monetary awards should also be

[14] This was just one of the brilliant moves of the Goldwater-Nichols Act that forced the military services to team together.

awarded for quality coordinating and collaborating work with other agencies. There must be processes designed to break the incentive for a collecting agency to withhold information for the purposes of being the first to report it. The goal should rather be to get it out to everyone and achieve consensus through competitive analysis on the meaning of the information.

These standardizations will not be easy, as there are strongly held policy differences between agencies. For example, DIA will not take adverse personnel action solely based on a failed polygraph test. On the other hand, the CIA can fire someone on the basis of a polygraph. The point here is not to propose what the standards should be, but to emphasize that it is critical to have some standardization so that data access can be accomplished across agencies lines without concern that agency idiosyncrasies will impede the process.

Ensure NCTC/DNI Offices Are Not Infected With Institutional Biases

The only way to get away from the serious problem of individual agencies not understanding or accepting the roles and missions of other CT organizations is to ensure the ODNI is staffed with individuals who are clearly in favor of equal access for all national CT centers. This is easier said than done. Many analysts advance in their careers biased toward the agencies that gave them trusted access. Their culture is one of obtaining information through contacts rather than equal access to data. They made their mark by creating trust and gaining information, not automatically based on their mission, but on personal relationships over the years. There are many of these talented career leaders who have served their agency and country well, but they may not be the right people to serve in the two new organizations that are mandated to share. If the IC is truly going to provide optimum all-source analysis, the people hired in the NCTC and ODNI must understand the capabilities of the entire IC and be dedicated to utilizing them. They will in-turn create and enforce new guidelines ensuring data access based on the problem sets one works rather than where one sits.

Revamp Attorney General Guidelines on NSA Data

The DNI should request that the Attorney General reexamine implementation guidance for EO 12333, as discussed earlier. This guidance needs to change, and if that means EO 12333 needs to be changed, then the President must be asked to modify it so that it does not hinder access to direct translation of NSA intercepts by national CT analysts. Senior decision makers must be made aware that one EO is being used as an excuse not to implement another EO that mandates that intelligence be shared.

Revamp FISA Access

JITF-CT has been formally pushing for direct data access to intelligence gathered through FISA for over a year. They took their case to the DNI who turned it over to the FISA panel established by the Patriot Act. JITF-CT has been waiting patiently for a decision that, as of the writing of this paper (June 2006), has yet to be made. The FISA panel should act without delay and grant this access not just to JITF-CT but to all the national CT centers based on the "need to know" argument laid out throughout this paper.

Data Mining Tools in a Central Database

Although the focus of this paper is on data access for the right people, it must be noted that granting access alone is not enough. A concerted effort must take place to create a standardized data mining tool able to search all CT databases so analysts can search through all the pertinent CT data the U.S. government possesses. The U.S. government is wasting resources if it allows the FBI to work on data mining tools for their databases, the CIA for theirs, the NSA for theirs, etc. Most of these agencies have multiple databases and search tools, but there is currently no powerful terrorism data mining tool for the CT community as a whole. Yet, the technology exists to connect these databases. Granted, just as connected databases allow analysts to more easily connect the dots, it also makes it easier for someone who has infiltrated our intelligence community to conduct espionage. The risk of espionage cannot be ignored. The very best technology available to audit and monitor must be part of the counterintelligence (CI) safeguards that need to be in full force to protect data as it is linked together. Robust CI safeguards are where the focus of data protection needs to be rather than limiting access to national CT analysts outside the collecting agency. *The intelligence community needs connected databases with equal access among those working the same problem sets and data mining tools to assist them. It is only then that the U.S. government will be fully optimizing its resources to uncover future plots that may be hidden away in the multitude of terrorism databases of the U.S. government.*

United Kingdom-Style Official Secrets Act

If, hypothetically, there were never any unauthorized disclosures, then the argument of the intelligence collectors would essentially go away. You would not have to worry about the national security impact of a disclosure. Foreign governments would learn that they could completely trust us with their information and spies would have confidence that what they passed to us would not be leaked. Because this seems to be the main concern, one would think there would be much focus on stopping these disclosures. Instead, the main focus continues to be limiting access to those very analysts tasked with trying to connect the dots.

To stop leakers, the United States needs a U.K.-style Official Secrets Act, which enacted strong laws, not just against spies, but against leakers and the media that publishes them. Moreover, the U.K. has a solid record for actually prosecuting those who violate the Act. Granted, this is much more difficult to achieve in the United States because of the near reverence with which the First Amendment is viewed. Yet, the simple truth is that it is normally impossible to uncover the source of a leak unless reporters are forced to reveal their sources.

The recent Judith Miller case provides a good example of some of the barriers law enforcement agencies run up against when trying to uncover leaks. As one official interviewed pointed out, Special Prosecutor Patrick Fitzgerald had to obtain a waiver from the Attorney General's office in order to get a subpoena. The waiver was necessary because Attorney General guidelines are such that in order to subpoena a reporter, a life-threatening situation has to exist. Those who want to stop such leaks might have hoped that Judith Miller's subpoena may serve to deter others from writing and publishing classified information. Evidence suggests otherwise. The Judith Miller subpoena did not stop Dana Priest and the Washington Post from disclosing an alleged secret CIA prison system in Eastern Europe. The New York Times decision to reveal the existence of an NSA

monitoring program conducted without FISA Court involvement came after Judith Miller had been subpoenaed.

These are just two events pulled from recent headlines, but there is a strong history of classified information being published in newspapers with impunity, even in cases that do not fall into the whistle blowing category. Strong laws against unauthorized disclosures need serious debate in this country especially in light of the fact that the main argument against sharing intelligence is that it will result in unauthorized disclosures. Also, toughening laws against the leakers themselves needs to occur. The fact that "Scooter" Libby is being prosecuted for lying instead of providing classified information to a reporter is testament to this fact.

The U.S. government should be fighting for a U.K. Official Secrets Act with the same vigor the current administration fought for the Patriot Act. Admittedly, the chances of passing this type of act are slim, at least in the short term. Although the House of Representatives Permanent Select Committee on Intelligence (HPSCI) held hearings on unauthorized disclosures last year, they went nowhere and received little attention. Committee staffers interviewed indicated there was no support for taking on this issue beyond the initial hearings. The Libby controversy, rather than opening the door to go after leakers, had the opposite effect of rallying First Amendment protection for the press, losing the support to take on this issue with the administration, and stifling the initiative of the Chairman of the HPSCI. Passing stronger unauthorized disclosure laws needs to be a long-term goal, but all the other measures proposed can be done now, under the mandates given to the DNI in the IRTPA. It cannot be emphasized enough that no matter how much progress is made on unauthorized disclosures, cleared analysts working the same problem sets as other agencies should have the same access and of course fall under the same security rules.

Executive Leadership

Everything in these recommendations, besides a U.K. style Official Secrets Act, is within the power of the DNI as laid out in the IRTPA. What is needed is leadership from the President and his appointees to make it a reality. That will not be easy as the data collector will always be able to go to the President and the DNI and say it is critical for certain information to remain "secure" and not be shared. They can and will persuasively argue that our national security is at stake. When decision makers are presented with this dilemma, they must be prepared to tell the collecting agency heads that they understand, but they still want all CT analysts in the national CT centers to have access to ensure we are fully optimizing the nation's counter terrorism analytical capability.

What to Guard Against?

The IC has a long history of protecting its information by creating special compartments within compartments to limit access. There is an expression for this trend that "behind every green door there is another green door."[15] Those who believe data access should not evolve any further will no doubt use this technique to circumvent any actions taken to grant equal access to those working the same problem sets. This phenomenon is already showing itself at the NCTC. It is imperative that the

[15] In the old days, a special compartment facility (places where the classified information is held) had green doors at the entrance.

DNI provide strong oversight of data access at the NCTC, and take bold actions to ensure the NCTC has access to all terrorism data as mandated in the IRTPA. If the NCTC succeeds, the DNI then should use it as the model for data access for the rest of the national CT centers.

Behind Every Green Door There is Another Green Door

Just as special interest groups circumvent special interest reform legislation by lobbying for loopholes or just by finding innovative ways around the legislation, the same is true for sharing intelligence data. This phenomenon can already be observed at the NCTC. The IRTPA calls for the NCTC to serve as the "primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorist and domestic counterterrorism."[16] The NCTC was given responsibility for "all" intelligence pertaining to terrorism over the objection of the CIA/DO. Despite being mandated in law and by Executive Order, the NCTC Director had to fight tooth and nail to ensure NCTC actually received "all" intelligence on terrorism.

And yet, NCTC personnel are told upon arrival that everyone is not going to have access to everything. CIA terrorism related information is divided into different categories and not all terrorism analysts have equal access. Those with the best access are almost exclusively reserved for those analysts that came to the NCTC from the CIA. This is wasting the value of the other CT agencies that U.S. Congress has funded to specifically provide for unique perspectives in the counter terrorism analytical process. What is even more disconcerting is how this author received testimonials that CIA circumvented non-CIA analysts serving in NCTC from having access to CIA's unreported terrorism data. Over time, NCTC CT analysts found increasing references to Lotus Notes e-mails when reading ops traffic. The CIA now appears to be communicating the "really good stuff" via an e-mail system (not available to everyone in the NCTC). If the revolution of data access is such that equal access to unreported data is given to the national CT centers, this green door syndrome will undoubtedly operate in full swing to stop CT centers from truly gaining equal access. The DNI first must stop this from happening, inside the NCTC. The NCTC needs to be the model that can ultimately lead the way for the other national CT centers: equal access with equal security safeguards.

The NCTC Must Succeed

As previously discussed according to the IRTPA, the NCTC exists to ensure that all the terrorism agencies are getting the intelligence they need to complete their mission.[17] The NCTC is failing at this and currently not in compliance with the law as laid out in the IRTPA. The majority of national CT centers do not have the data they need to carry out their activities and do alternative analysis. Moreover, it remains to be seen whether the NCTC as an organization will maintain the access it gained if the collectors in CIA succeed in circumventing much of the access of non-CIA analysts

[16] Intelligence Reform and Terrorism Prevention Act of 2004, Subtitle B, Sec 1021.

[17] Ibid., Subtitle B, Sec 1011.

through the use of Lotus Notes or other means.[18] It is vital that the NCTC be made to succeed as the model for gaining access to other national CT centers through the use of standardized safeguards. This will not occur unless the DNI forces this change. He has not only the authority under the IRTPA, but also the mandate from the President. The DNI must not let ambiguities in the language, such as "to the extent possible," hinder him. The first step is for the DNI to define and/or validate the missions of the national CT centers.

If and when equal access is mandated for the national CT centers, the collectors of data could in turn try to limit access by taking away access already given to analysts at the NCTC and the CTC. In other words, the DNI must not allow the collectors to agree to give the national CT centers everything they give NCTC and CTC and then find innovative ways to give NCTC and CTC less. There is a very real danger that a major step forward could turn into two major steps backwards. Although this may sound far-fetched with all the publicity for better sharing, it is not. The DNI must do whatever is necessary to take away from the collecting agency the power to control data access.

Conclusion

We are running out of time for national CT analysts to have to continue bartering for data access. No matter what the DNI mandates, he will need to watch out for the innovative ways in which agencies may try to circumvent his actions as outlined above. The DNI needs to ensure the building of a central database with powerful data mining software. It must have highly capable security features and powerful auditing tools as its unauthorized use will be a grave security threat. Instead of saying that we cannot share because of risk of unauthorized disclosures, the DNI must say we are going to ensure data access to the right people and we are going to deal more aggressively to prevent unauthorized disclosures than ever before. The effective operations security (ability to keep their operations secret) of al-Qaida should not be an example for the U.S. government to go to extremes to limit access to intelligence data. Rather, al-Qaida should be the example of why the U.S. CT community needs to connect their CT centers and intelligence assets in the way al-Qaida connects their networks. They were successful on 9/11 in part because they were networked across the world while our intelligence services were not even networked domestically. The U.S. government must transform the IC so that the best analysts across all of our unique counter terrorism agencies are looking at the best intelligence possible there by bringing all the relevant perspectives to bear on the problem set. It is in this way that the IC will team together to "connect the dots" and uncover what al-Qaida and others are working so hard to keep secret.

Currently, we do not have an IC; rather, we have a loose confederation of intelligence components. To truly turn it into a community, the DNI must outmaneuver those who oppose this goal. Coordination and collaboration are not group efforts when the groups are operating with different data sets and the organization that has the best access cannot discuss its data with the other groups. The United States spends a huge amount of dollars on intelligence activities which naturally should come with taxpayer expectations. The public would be outraged if it realized that only a very small group in the intelligence community gets all the data of significance and the rest of the community is

[18] Initial signs are not encouraging. For example, the head of intelligence sharing at NCTC told this author that he believes terrorism data should be centralized at NCTC with no further access to unreported information.

operating nearly in the blind. Analysts must stop spending so much energy in obtaining information that the U.S. government already has. Instead, their focus needs to be on assessing all data in their problem set to uncover secrets not yet discovered.

Those who are against sharing have precedent, culture, human nature, and power on their side. The DNI must break through all these barriers. Once an independent body is making the access decisions, then it will be incumbent upon the CT centers to both prove their value and their ability to safeguard the information. Analysts at the national CT centers are equally dedicated to connecting dots and maintaining security. The tremendous cumulative value that comes with the different perspectives that each analyst brings based on his or her background and the roles and mission of his or her particular agency cannot be overstated. There are many tough roads ahead, and access to unreported information is just one of them. But how can the United States solve the huge issue of getting sensitive credible threat information to local authorities who lack clearances when they cannot even share data between community-cleared analysts? The U.S government must be relentless in its pursuit to get all the national CT centers looking at the same data set in order to connect the dots in time to prevent another horrific attack.