Order Code RL31292

Report for Congress
Received through the CRS Web

Intelligence to Counter Terrorism: Issues for Congress

Updated May 27, 2003

Richard A. Best, Jr.
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

Intelligence to Counter Terrorism: Issues for Congress

Summary

For well over a decade international terrorism has been a major concern of the U.S. Intelligence Community. Collection assets of all kinds have long been focused on Al Qaeda and other terrorist groups. Intensive analytical expertise has been devoted to determining such groups' memberships, locations, and plans. Intelligence agencies had been acutely aware of the danger for years. In February 2001, Director of Central Intelligence (DCI) George Tenet publicly testified to Congress that "the threat from terrorism is real, it is immediate, and it is evolving." Furthermore, "[Osama] bin Ladin and his global network of lieutenants and associates remain the most immediate and serious threat."

Nevertheless, the Intelligence Community gave no specific warning of the September 11, 2001 attacks. Although all observers grant that terrorist groups are very difficult targets and that undetected movements of small numbers of their members in an open society cannot realistically be prevented, serious questions remain. An extensive investigation by the two intelligence committees of the September 11 attacks was undertaken in 2002. Although the final report is not yet public, the committee members found that the Intelligence Community, prior to 9/11, was neither well organized nor equipped to meet the challenge posed by global terrorists focused on targets within the U.S. A separate independent commission was established in early 2003 to take another look at the events preceding September 11.

Counterterrorism is highly dependent upon human intelligence (humint), the use of agents to acquire information (and, in certain circumstances, to carry out covert actions). Humint is one of the least expensive intelligence disciplines, but it can be the most difficult and is undoubtedly the most dangerous for practitioners. Mistakes can be fatal, embarrass the whole country, and undermine important policy goals. Congress makes decisions regarding the extent to which the importance of humint outweighs the inherent risks.

Countering terrorism requires close cooperation between law enforcement and intelligence agencies; some terrorists will need to be brought to justice in courts, but others are dealt with by military forces or covert actions. In recent years, important steps have been taken to encourage closer cooperation between the two communities, but some believe terrorist acts may have been facilitated by continuing poor information exchanges between intelligence and law enforcement agencies and by blurred lines of organizational responsibility. Congress will oversee the implementation of the evolving relationship that affects important principles of law and administration, and may choose to modify the roles and missions of intelligence and law enforcement agencies.

Military operations to counter terrorism are dependent on the availability of precise, real-time intelligence to support bombing campaigns using precision guided munitions. The linkage between sensor and "shooters" will be crucial as will access to global geospatial databases. As defense transformation progresses, Congress will also oversee the development of increased intelligence support to military operations including, especially, counterterrorist missions.

Contents

Intelligence to Counter Terrorism: Issues for Congress

Introduction

The struggle against international terrorism places new and difficult demands on the U.S. Intelligence Community. Acquiring information about the composition, location, capabilities, plans, and ambitions of terrorist groups is an enormous challenge for intelligence agencies; meeting this challenge requires different skills than were needed to keep informed about the capabilities and intentions of Communist governments. At the same time, requirements continue for coverage of geopolitical developments around the world and other transnational issues such as narcotics smuggling.

Observers point to several major challenges that the Intelligence Community will likely encounter in supporting the counter terrorist effort.

- First is **a renewed emphasis on human agents**. Signals intelligence and imagery satellites have their uses in the counterterrorism mission, but intelligence to counter terrorism depends more on human intelligence (humint) such as spies and informers. Any renewed emphasis on human intelligence necessarily will involve a willingness to accept risks of complicated and dangerous missions, and likely ties to disreputable individuals who may be in positions to provide valuable information. Time and patience will be needed to train analysts in difficult skills and languages.

- Second, terrorist activities pose **significant analytical challenges**. In addition to acquiring analysts with esoteric language skills, intelligence agencies must develop expertise in many third world areas that had been of peripheral concern in years past. Much of the data available will be in open, unclassified sources that intelligence agencies have often neglected.

- Third is **the closer relationship between intelligence and law enforcement agencies**. In counterterrorism efforts, intelligence agencies work alongside law enforcement agencies that have far different approaches to gathering evidence, developing leads, and maintaining retrievable databases. Policies and statutes are being modified to facilitate a closer relationship between the two sets of agencies, but closer cooperation has raised difficult questions about

using intelligence agencies in the U.S. and about collecting information regarding U.S. persons.

- Finally, military operations against terrorists will reenforce requirements for collecting and transmitting **precise intelligence to military commanders** or operators through secure communications systems in real time. The growing reliance of military operations on the availability of precise intelligence is well understood, but the availability of collection platforms such as reconnaissance aircraft, unmanned aerial vehicles, and reconnaissance satellites has been limited throughout much of the past decade. Such platforms are especially important for counterterrorist operations.

In large measure, meeting these challenges will be the responsibility of executive branch officials. The primary role for Congress will be to decide appropriate levels of budgetary resources and to oversee Intelligence Community efforts to ensure that resources are well managed and that the nation's intelligence needs are met. Some observers believe that Congress has special responsibilities to provide a clear statutory framework to guide the unprecedented and uncertain evolution of intelligence-law enforcement relationships. Such a framework is necessary, they suggest, to minimize chances for a failure of the campaign against terrorists or, alternatively, serious erosion of the protections of individual liberties that have evolved over many centuries.

In the aftermath of September 11, 2001, Congress moved rapidly to provide intelligence agencies with expanded authorities and increased funding to support counterterrorism. In the year 2002, congressional intelligence committees investigated the background of the September attacks and recommended legislation to reorganize the U.S. Intelligence Community. Vast intelligence assets were deployed in support of military operations in Iraq, and there are continuing requirements in Afghanistan. Programs likely will be established to support the long-term struggle against terrorism and necessary budgetary resources identified. Intelligence support to the Department of Homeland Security is a key concern and one that remains under review.

In November 2001, one media account suggested that a major reorganization of the Intelligence Community might be under consideration by the executive branch.[1] Members of the two intelligence committees released a number of recommendations in December 2002 to strengthen management of intelligence activities.[2] The legislative future of such proposals is uncertain, however. Whatever the organizational relationships, intelligence for counterterrorism will be affected by the need for good humint, analysis, close ties to law enforcement agencies, and for capabilities to support military operations with precise locating data.

---

[1] See Walter Pincus, "Intelligence Shakeup Would Boost CIA; Panel Urges Transfer of NSA, Satellites, Imagery From Pentagon," *Washington Post*, November 8, 2001, A1.

[2] See James Risen and David Johnston, "Threats and Responses: the Congressional Report; Lawmakers Want Cabinet Position for Intelligence," *New York Times*, December 8, 2002, p.1.

Background

During the Cold War, terrorism was not a major intelligence priority and, in many cases, terrorist groups were perceived as acting on behalf of, or at least with important support by, Communist parties. The focus was on the other superpower and not terrorism *per se*. Nevertheless, the Intelligence Community has long devoted significant resources towards the terrorist threat. As early as 1986, a Counterterrorism Center (CTC), comprised of officials from various intelligence and law enforcement agencies, was established within the Operations Directorate of the Central Intelligence Agency (CIA) to pull together information on international terrorism from all sources and devise counterterrorism plans. After the fall of the Soviet Union and the Warsaw Pact, terrorism was perceived with even greater concern, especially as U.S. military forces and installations repeatedly were attacked by terrorist groups as in the 1996 Khobar towers barracks in Saudi Arabia, the August 1998 bombing of U.S. embassies in Kenya and Tanzania, and the attack on the USS Cole in October 2000.

Public statements by senior intelligence officials affirm that the threat to the United States posed by international terrorism was understood well before September 11, 2001. In February 2001, the Director of Central Intelligence (DCI) George Tenet, in prepared testimony before the Senate Intelligence Committee, stated: "the threat from terrorism is real, it is immediate, and it is evolving. State sponsored terrorism appears to have declined over the past five years, but transnational groups — with decentralized leadership that makes them harder to identify and disrupt — are emerging." Furthermore, "[Osama] bin Ladin and his global network of lieutenants and associates remain the most immediate and serious threat."[3] In this testimony, Tenet stated that Al Qaeda and other terrorist groups will continue to plan to attack this country and its interest and have sought to acquire dangerous chemical agents and toxins as well as nuclear devices.[4]

The creation of CIA's Counterterrorism Center (CTC) was an early effort to bring together disparate data on terrorist activities. The CTC has not been considered a complete success;[5] collection on terrorist groups did not become an overriding priority and, although the Federal Bureau of Investigation (FBI) had representatives in the CTC, the relationship with the law enforcement community did not evolve as

---

[3] Statement by Director of Central Intelligence George J. Tenet before the Senate Select Committee on Intelligence on the "Worldwide Threat 2001: National Security in a Changing World" (as prepared for delivery), 7 February 2001.

[4] "Worldwide Threat — Converging Dangers in a Post 9/11 World," Testimony of Director of Central Intelligence George J. Tenet Before the Senate Select Committee on Intelligence, February 6, 2002.

[5] For the background to the establishment of the CTC, see Duane R. Clarridge with Digby Diehl, *A Spy for All Seasons: My Life in the CIA* (New York: Scribner, 1997), especially pp. 319-429. See also Robert Baer, *See No Evil: the True Story of a Ground Soldier in the CIA's War on Terrorism* (New York: Crown Publishers, 2002), pp. 84-86. For a description of its more recent functioning, see Paul R. Pillar, *Terrorism and U.S. Foreign Policy* (Washington: Brookings Institution, 2001), especially pp. 110-123.

fully as had been hoped. Media accounts indicate that the CTC doubled in size in the month following the attacks.[6]

It is difficult to judge how successful the overall counterterrorism effort has been. The September 11, 2001 attacks were successful, but other terrorist plans have been thwarted although few details have been revealed. A multi-faceted attack on the Los Angeles airport and other U.S.-related targets to coincide with millennium celebrations in January 2000 was foiled as a result of a chance apprehension of an individual with a car loaded with explosives by an alert Customs Service official.[7] Attacks on U.S. embassies and facilities in Paris, Singapore, and other parts of the world have reportedly been thwarted because of intelligence leads.

Inevitably there has been public discussion of the question of whether September 11 was an "intelligence failure."[8] A joint investigation by the House and Senate intelligence committees was undertaken in 2002 by a Joint Inquiry Staff. The final report will not be publicly available until mid-2003, but a number of findings and recommendations were made public in December 2002 that described inadequacies in the organization of the Intelligence Community.[9] In the FY2003 Intelligence Authorization Act (P.L. 107-306) Congress also established an independent commission to review the review the evidence developed by government agencies surrounding the 9/11 attacks. The commission has 18 months to submit its report.

Some observers have suggested comparisons to the investigations that were undertaken during and after World War II concerning the Japanese attack on Pearl Harbor.[10] Those investigations were viewed by many observers as politicized — either seeking or deflecting mistakes by the Roosevelt Administration. By the time of the conclusion of the congressional investigation in July 1946, almost a year after the end of the war, the public was concentrating on other issues and, as a result, there was little political fall-out.[11] The investigations did, however, indicate the need for

---

[6] Walter Pincus, "CIA Steps Up Scope, Pace of Efforts on Terrorism," *Washington Post*, October 9, 2001, p. A4.

[7] Neil King Jr. and David S. Cloud, "Casting a Global Net, U.S. Security Survived a Rash of Millennial Plots," *Wall Street Journal*, March 8, 2000; also, Laura Mansnerus and Judith Miller, "Bomb Plot Insider Details Training," *New York Times*, July 4, 2001, p. A1.

[8] An oft-cited analysis of the phenomenon of intelligence failures is Richard K. Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics*, October, 1978.

[9] See CRS Report RL31650, *The Intelligence Community and 9/11: Congressional Hearings and the Status of the Investigation*, by Richard A. Best, Jr., updated January 16, 2003.

[10] These are described in Martin V. Melosi, *The Shadow of Pearl Harbor: Political Controversy over the Surprise Attack, 1941-1946* (College Station, Texas: Texas A&M University Press, 1977).

[11] None of the various Pearl Harbor investigations definitively resolved the issue of the "blame" for Pearl Harbor. In particular, controversy has persisted over the roles of two senior U.S. officers at Pearl Harbor, Rear Admiral Husband E. Kimmel, USN and Major

(continued...)

better coordination among intelligence agencies and between intelligence agencies, policymakers, and military commanders.

It is argued that "lessons" of Pearl Harbor, as viewed by senior congressional and executive branch officials, laid the groundwork for the establishment of a national intelligence effort by the National Security Act of 1947. Similarly, the investigation of the events leading up to the September 11 attacks might lay the groundwork for a new relationship between intelligence and law enforcement.

In the immediate wake of 9/11, Congress passed the USA Patriot Act, a principal purpose of which was to remove perceived restrictions on closer law enforcement-intelligence cooperation in order to support counterterrorist efforts.[12] Modifications to the Foreign Intelligence Surveillance Act (FISA) for the same purpose were enacted shortly thereafter as part of the FY2002 Intelligence Authorization Act (P.L. 107-108), and further changes are being considered in 2003.

The need to integrate intelligence and law enforcement information greatly influenced the deliberations that resulted in the establishment of the Department of Homeland Security (DHS) in early 2003. This legislation envisioned an analytical directorate in DHS that would be the center of an integrative effort based on information from intelligence and law enforcement sources. The executive branch, however, has created a separate Terrorist Threat Integration Center (TTIC), under the direction of the DCI, that began operations in May 2003.

At the same time, a number of observers have expressed serious concerns about closer ties between intelligence and law enforcement agencies and, especially, about the use of intelligence gathering techniques against U.S. citizens and resident aliens. The passage of the USA Patriot Act and related legislation in the wake of 9/11 has been criticized as a fundamental weakening of civil liberties protections. Further legislative initiatives to align law enforcement and intelligence efforts more closely are likely to result in greater opposition.

Aside from the investigation into the background of the September 11 attacks, intelligence agencies will be adapting their efforts to the requirements of the campaign against terrorism. Renewed emphasis is being placed on human intelligence, on improved analysis, on cooperation with law enforcement agencies, and on ensuring that real-time intelligence about terrorist activities reaches those who can most effectively counter it.

---

[11] (...continued)
General Walter C. Short, USA, who, some believe, were unfairly held responsible for shortcomings of Roosevelt Administration officials. Almost fifty-nine years after the Japanese attack, the National Defense Authorization Act of FY2001 expressed the sense of Congress that both officers had performed their duties "competently and professionally" and asked that the retirement status of Kimmel and Short be upgraded posthumously (P.L. 106-398, sec. 546).

[12] See CRS Report RL31377, *The USA Patriot Act: A Legal Analysis* by Charles Doyle.

Humint Collection

Many observers believe that intelligence required for the campaign against terrorism will require significant changes in the human intelligence (humint) collection effort. The CIA's Operations Directorate is responsible for the bulk of humint collection although the Defense Humint Service within DOD is a smaller entity more directly focused on military-related issues. Overall budget requirements for humint are dwarfed by the major investment required for satellites and signals intelligence collection. Humint, however, undoubtedly can be dangerous for those involved and it is, of course, for many in the media and the general public the core intelligence discipline.[13]

Both the emphasis on humint and on the exchange of data between intelligence and law enforcement agencies will influence the evolution of the U.S. Intelligence Community in the coming decade. These two efforts will not in themselves have major budgetary implications — humint is both difficult and dangerous, but not necessarily expensive and information exchanges between agencies ordinarily involve only information technology costs. However, placing priorities on these two aspects of the intelligence effort will almost inevitably detract from other missions and disciplines. In the view of many observers there may be a tendency to give less emphasis to traditional intelligence collection and analysis regarding foreign political, economic, and military developments. Whereas to some extent intelligence analysts experienced in looking at foreign policy, economic, and defense issues can shift from one country to another, it may be more difficult for an analyst to turn from issues of diplomacy, economics, and warfare to the study of obscure terrorist groups that may be involved in religious indoctrination or various criminal fund-raising activities.

Although humint is not in itself an expensive discipline, it requires large amounts of support and an awareness by senior officials of possible negative consequences. Potential complications, including imprisonment of U.S. agents in foreign countries and loss of friendly lives, have to be given careful consideration. Major diplomatic embarrassment to the United States can result from revelations of covert efforts, especially those that go awry; such embarrassment can jeopardize relationships that have been developed over many years.

---

[13] Humint collection must be distinguished from covert actions even though the two efforts may be undertaken by the same people or organizations. In the aftermath of September 11, the CIA's Special Activities Division rapidly mounted covert paramilitary operations in Afghanistan. Media accounts suggest that this effort is being mounted by retired military specialists brought back into government to supplement much smaller numbers of longtime CIA officials with experience in the region. Much of their assignment reportedly involved identifying specific targets for airborne attack and other liaison with Northern Alliance units. See Bob Woodward, "Secret CIA Units Playing a Central Combat Role," *Washington Post*, Nov. 18, 2001, p.A1. For background on covert actions, see CRS Report 96-844, *Covert Action: An Effective Instrument of U.S. Foreign Policy?*, by Richard A. Best, Jr.

Collecting humint to support the counterterrorism effort will require significant changes in the work of intelligence agencies.[14] Terrorists do not usually appear on the diplomatic cocktail circuit nor in gatherings of local businessmen. In many cases they are also involved in various types of criminal activities on the margins of society. Terrorist groups may be composed almost wholly of members of one ethnic or religious group. They may routinely engage in criminal activities or human rights abuses. Developing contacts with such groups is obviously a difficult challenge for U.S. intelligence agencies; it requires long-lead time preparation and a willingness to do business with unsavory individuals. It cannot in many cases be undertaken by intelligence agents serving under official cover as diplomats or military attaches. It may require an in-depth knowledge of local dialects and customs. Furthermore, the list of groups around the world that might at some point in the future be involved in terrorist activities is not short; making determinations of where to seek agents whose reporting will only be important under future eventualities is a difficult challenge with the risk of needlessly involving the U.S. with corrupt and ruthless individuals.

Critics of the current U.S. humint collection effort point to these and other institutional problems. One report quotes a former CIA official:

> The CIA probably doesn't have a single truly qualified Arabic-speaking officer of Middle Eastern background who can play a believable Muslim fundamentalist who would volunteer to spend years of his life ... in the mountains of Afghanistan....[15]

Some observers have claimed that CIA personnel in key positions do not know the major languages of the areas for which they are responsible.[16] A former CIA official stationed in Tajikistan in the early 1990s recalled that "As the civil war in Afghanistan started to boil, I repeatedly asked for a speaker of Dari or Pashtun, the two predominant languages in Afghanistan, to debrief the flood of refugees coming across the border into Tajikistan. They were a gold mine of information. We could have even recruited some and sent them back across the border to report on Afghanistan. I was told there were no Dari or Pashtun speakers anywhere. I was also

---

[14] A discussion of current weaknesses in the CIA's humint effort is found in Seymour M. Hersh, "What Went Wrong," *New Yorker*, October 8, 2001. Hersh claims that CIA has "steadily reduced its reliance on overseas human intelligence and cut the number of case officers abroad;" in recent years CIA "has relied on liaison relationships — reports from friendly intelligence services and police departments around the world — and on technical collection systems." Page 35.

[15] Reuel Marc Gerecht, "The Counterterrorist Myth," *Atlantic Monthly*, July/August 2001. The former CIA Inspector General, L. Britt Snider (who has also recently been named staff director of the joint investigation of the September 11 attacks by the two intelligence committees), concluded that the CIA "has a relatively unstructured assignment process which seems tilted more towards satisfying the preferences of employees than mission needs. It has a personnel evaluation process that defies any effort to weed out poor performers." "A Message from the Inspector General, Central Intelligence Agency, January 19, 2001,"reprinted on the Web site of the Federation of American Scientists [http://www.fas.org].

[16] *E.g.*, Richard Perle, a Defense Department consultant, quoted by Ken Adelman, "Facing the Enemy," *Washingtonian*, November 2001, p. 33.

told the CIA no longer collected on Afghanistan, so those languages weren't needed."[17] Although such broad claims are disputed and cannot be evaluated without access to classified information, it is not clear what steps the Intelligence Community has taken to realign its humint operations. Developing a humint collection strategy under these circumstances is a difficult challenge for the Intelligence Community, especially for the CIA's Operations Directorate, the FBI, and the smaller Defense Humint Service. Observers suggest the need for a series of policy decisions involved in a reorientation of humint collection.

- A move towards greater reliance on non-official cover (NOC). Non-official cover means that agents are working as employees or owners of a local business and thus are removed from the support and protections of American embassies that would be available if the agent had cover as a U.S. government official of a non-intelligence agency. If the agent must be seen as engaged in business, considerable time must be devoted to the "cover" occupation. Providing travel, pay, health care, administrative services, etc. is much more difficult. The agent will not have diplomatic immunity and cannot be readily returned to the U.S. if apprehended in the host country. He or she may be subject to arrest, imprisonment, or, potentially, execution. There is a potential for agents working in businesses to become entangled in unethical or illegal activities — to "go into business for themselves" — that could embarrass the U.S. and detract from their official mission.[18]

- Requirements for U.S. intelligence agents with highly developed skills in foreign languages are difficult to meet. Few graduates of U.S. colleges have such skills and language education is expensive. Recruiting U.S. citizens who have ethnic backgrounds similar to members of the societies in which the terrorist groups operate may subject individuals to difficult pressures especially if the agent has family in the targeted area. The House Intelligence Committee reported in September 2001 that the Intelligence Community's "most pressing need is for greater numbers of foreign language-capable intelligence personnel, with increased fluency in specific and multiple languages. The Committee has heard repeatedly from both military and civilian intelligence producers and consumers that this is the single greatest limitation in intelligence agency personnel expertise and that it is a deficiency throughout the Intelligence Community."[19]

---

[17] Baer, *See No Evil*, pp. 164-165.

[18] The need to reorient the humint collection effort to a greater reliance on non-official cover is discussed by Gregory F. Treverton, a senior intelligence official in the Clinton Administration, *Reshaping National Intelligence for an Age of Information* (New York: Cambridge University Press, 2001), pp. 152-157.

[19] U.S. Congress, 107th Congress, 1st session, House of Representatives, Permanent Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2002*, H.Rept.

(continued...)

- It is administratively difficult to develop resources throughout the world over a long period of time and costs are higher than adding intelligence staff to embassies. Few observers could have predicted the intense U.S. concern with Somalia, Kosovo, or Afghanistan that eventually developed. Ten years from now there may be a whole set of challenges from groups that no one today is even aware of.

In short, reorienting humint collection to give significantly greater attention to terrorist or potentially terrorist groups would have important administrative implications for the Intelligence Community. While budgetary increases would not necessarily be dramatic given the size of the existing intelligence budget (even paying hundreds of human agents would be far less costly than deploying a satellite), the infrastructure needed to train and support numerous agents serving under non-official cover would grow significantly. Extensive redundancy would be required to cover terrorist groups that may never pose significant threats to U.S. interests.

With such considerations in mind, the Senate Intelligence Committee, in its report accompanying the FY2004 Intelligence Authorization bill (S. 1025), noted interest among some Members in more vigorous humint collection, "especially unilateral — collection — under non-official cover and from non-traditional HUMINT 'platforms.' " The Committee further noted that some observers have even suggested "the need for the creation of a small, highly specialized semi- or fully-independent HUMINT entity charged with collecting against non-traditional targets and rogue states that traditionally have proven highly resistant to HUMINT penetration involving traditional official-cover operations." The Committee did not endorse this concept but urged "diligent effort and new approaches to HUMINT management within existing agency components."[20]

A central issue for Congress is the extent to which it and the public are prepared to accept the inherent risks involved in maintaining many agents with connections to terrorist groups. Statutory law[21] requires that congressional intelligence committees be kept aware of all intelligence activities; unlike the situation in the early Cold War years when some intelligence efforts were designed to be "deniable," it will be difficult for the U.S. Government to avoid responsibility for major mistakes or ill-conceived efforts of intelligence agencies. Although there is a very widespread consensus that Al Qaeda poses a threat to all Americans and to fundamental American interests, it cannot be assumed that the U.S. public, or Members of Congress, will view other groups in the same light. Intelligence professionals recall that earlier associations with anti-communist elements in Central America came

---

[19] (...continued)
107-219, September 26, 2001, pp. 18-19.

[20] U.S. Congress, 108th Congress, 1st session, Senate, Select Committee on Intelligence, *Authorizing Appropriations for Fiscal Year 2004 for Intelligence and Intelligence-Related Activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System,* S.Rept. 108-44, May 8, 2003, pp. 23-24.

[21] 50 USC 413(a)(1). Separate provisions require notice of presidential findings authorizing covert actions (50 USC 413b).

under sustained public criticism (because some of the anti-communists were guilty of human rights violations and because they were, or appeared to be, propping up reactionary and oppressive regimes). These criticisms came to be shared by many Members of Congress and, as a result, intelligence agencies perceived that they were operating under excessive scrutiny and a cloud of suspicion for many years.[22] The direct attacks on the U.S. homeland on September 11, 2001 may well have produced a willingness on the part of the American public to accept greater risks, but intelligence professionals will undoubtedly be concerned to ensure that the work of their agencies not be jeopardized by shifts in public opinion.

Analysis

Terrorist activities present intelligence analysts with major challenges. First, there must be an awareness of the social, ideological, and political environment in which terrorist movements develop. Such awareness usually requires detailed knowledge of geographic, ethnic, religious, economic, and political situations in obscure regions. There is no ready supply of analysts with command of such skills except perhaps among recent emigrants who may have complex ties to their homelands. Moreover, areas of concern are likely to shift over time. As one longtime observer has noted, such analysts could "serve their whole careers without producing anything that the U.S. government really needs, and no good analyst wants to be buried in an inactive account with peripheral significance."[23]

Much of the information required to analyze terrorist environments derives from extensive study of open source documents — newspapers, pamphlets, journals, books, religious tracts, etc. Some observers believe that the Intelligence Community overly emphasizes sophisticated technical collection systems and lacks a comprehensive strategy for collecting and exploiting such open source information (osint).[24] Although efforts are underway by intelligence agencies to expand the use of osint, many observers believe that intelligence agencies should continue to concentrate on the collection and analysis of secret information. In this view, the Intelligence Community should not attempt to become a government center for research that can more effectively be undertaken by think tanks and academic institutions.

---

[22] Many of the statutory restrictions on intelligence activities imposed in response to public criticism have, nonetheless, been widely accepted and congressional oversight of intelligence agencies is now routine.

[23] Richard K. Betts, "Fixing Intelligence," *Foreign Affairs*, January/February 2002, p. 48.

[24] The principal advocate of greater use of open source information is Robert D. Steele, *On Intelligence: Spies and Secrecy in an Open World* (Fairfax, Virginia: AFCEA International Press, 2000). A recent media account suggests that U.S. Special Forces sent on a mission to destroy an Al Qaeda tunnel were surprised by the vast size of the compound and the amount of supplies; in fact, according to the report, the complex had been described in detail on an unclassified website months earlier. See Steve Vogel, "Al Qaeda Tunnels, Arms Cache Totaled," *Washington Post*, February 16, 2002, p. A27.

Once a terrorist group hostile to American interests has been identified, the Intelligence Community will be called upon to focus closely upon its membership, plans, and activities. Many collection resources will be targeted at it and much of the information will be classified and highly sensitive. The most challenging problem for analysts at this point is to attempt to discern where the terrorists will strike and through what means. Open societies are inevitably vulnerable to terrorists, especially those persons willing to commit suicide in the process of seeking their goals. The skills necessary to anticipate the unpredictable are extremely rare; some suggest a useful approach may be to assemble a "war room" comprised of a number of analysts to sift through all available data. Such an effort was created to follow Al Qaeda but did not foresee September 11. The bottom line is that anticipating such attacks is intellectually difficult; hiring more people and spending more money do not guarantee success.[25]

Others suggest greater reliance on outside consultants or an intelligence reserve corps when terrorist threats become imminent. Such an approach might also allow agencies to acquire temporarily the services of persons with obscure language skills. While there are security problems involved in bringing outside experts into a highly classified environment, this may be one approach that can provide needed personnel without unnecessarily expanding the number of government analysts.

In regard to analysis, major issues for Congress include holding intelligence agencies responsible for the quality of their work, the effective and efficient use of open source information, and the appropriate use of outside consultants. Analytical judgment is not easily mandated or acquired; leadership is key, along with accountability and a willingness to accept that even the best analysts cannot foresee all eventualities.

---

[25] Ibid., p. 58. Betts makes the interesting point that "expertise can get in the way of anticipating a radical departure from the norm." (P. 49) Terrorists succeed by undertaking actions that are unprecedented or, to American eyes, irrational. Thus, trained analysts with years of experience may be less inclined to "think outside the box" although ignorance of the terrorist group's composition and goals would not guarantee unique insights.

Intelligence-Law Enforcement Cooperation

In the past, the Intelligence Community focused on threats from the military forces of hostile countries and in large measure left terrorism to law enforcement agencies, especially the Federal Bureau of Investigation (FBI). Since the end of the Cold War in the early 1990's steps have been taken both by the executive branch and Congress to encourage closer coordination between the two communities. This effort was significantly expanded by P.L. 107-56, the USA Patriot Act, enacted in the wake of the 2001 attacks.

A recurring concern reflected in reports about the activities of those involved in the September 11 attacks has been the perception that information about possible terrorist involvement of individuals may not be available to immigration and law enforcement officials who encounter the individuals. There has not been a centralized database containing intelligence information by which individual names could be checked. Although there are many potential concerns about the establishment of centralized databases, most observers see the need to ensure that law enforcement agencies, including those of states and localities, have better access to information acquired by intelligence agencies about potential terrorist activities.[26]

Among some observers a major concern has been the Foreign Intelligence Surveillance Act. FISA was enacted in 1978 to establish a system for authorizing surveillance to collect information related to national security concerns. The process for obtaining a warrant under FISA differs from that for obtaining a warrant for criminal activities; there are different procedures and special FISA courts. The fundamental purpose is to provide judicial branch overview of a process that could be abused by zealous investigators. Enactment of FISA resulted from congressional concern about instances of politically-motivated surveillance efforts directed at U.S. citizens and residents. Over the years there have been a number of modifications to FISA to extend its procedures to cover physical searches as well as to cover new communications technologies.[27]

FISA procedures, however, have been blamed by some for restraining efforts to track foreign terrorists.[28] They cite, for instance, the inability of the FBI in August

---

[26] See CRS Report RL31019, *Terrorism: Automated Lookout Systems and Border Security: Options and Issues*, by William J. Krouse and Raphael F. Perl.

[27] See CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance*, by Elizabeth B. Bazan.

[28] See U.S., General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters is Limited*, GAO-01-780, July 2001. Also, John F. Harris and David A. Vise, "With Freeh, Mistrust was Mutual; Relations Soured over FBI's Role: For or Against Administration?" *Washington Post*, January 10, 2001, p. A1. Former DCI R. James Woolsey has claimed information about the 1993 World Trade Center bombing, whose perpetrators had ties to foreign terrorists, was not made available to intelligence agencies by the Justice Department. R. James Woolsey, "Blood Baath: the Iraq Connection," *New Republic*, September 24, 2001, p. 20. On the other hand, one federal investigator claimed that in trying to track down those responsible for the

(continued...)

2001 to obtain a FISA warrant for one individual, Zacarias Moussaoui, who was reportedly connected to an Algerian terrorist group.[29] After September 11, a warrant was obtained and Moussaoui's computer was found to contain information that suggested some involvement with terrorist activities. In the aftermath of the September 11 attacks, Congress passed modifications to FISA in the USA Patriot Act (P.L. 107-56) and in the FY2002 Intelligence Authorization Act (P.L. 107-108). Further changes have been proposed in the 108th Congress.[30] These initiatives reflect a determination to adapt FISA to the current international environment in which international terrorists may operate within and outside U.S. borders.

The new Department of Homeland Security that began operations in early 2003 has the statutory responsibility of using both intelligence and law enforcement information to provide assessments of terrorist activities and threats. The Homeland Security Act (P.L. 107-206) established within DHS an intelligence analysis directorate designed to integrate intelligence and law enforcement information relating to potential or actual terrorist threat to the United States. Subsequently, the Administration announced the establishment of a separate Terrorist Threat Integration Center under the direction of the DCI, which is to perform essentially those functions. There are ongoing discussions regarding the respective roles of DHS and TTIC.[31]

Placing emphasis on law enforcement by the Intelligence Community will have major implications for U.S. foreign policy. Over the years the U.S. government has maintained good relations, based on shared appreciation of common interests, with many governments whose legal systems are far different from our own. In some cases the U.S. has chosen to accept the fact that a foreign government may shield narcotics smugglers or members of groups the U.S. considers terrorist and to try to build a relationship of mutual interests with the country in the hope that its involvement with terrorists will eventually abate. Such a policy inevitably runs counter to the ethos of law enforcement agencies seeking to apprehend suspected criminals and put them on trial. Reportedly senior FBI officials during the Clinton Administration sought better cooperation from Saudi Arabia in prosecuting terrorists responsible for the Khobar Towers attack and resented a lack of support from State

---

[28] (...continued)
February 1993 attack, he "had zero cooperation from the intelligence community, zero." Quoted in Evan Thomas, "The Road to Sept. 11," *Newsweek*, October 1, 2001, p. 38.

[29] David Johnston and Philip Shenon, "F.B.I. Limited Inquiry of Man Now a Suspect in the Attacks," *New York Times*, October 6, 2001; James Risen, "In Hindsight, C.I.A. See Flaws that Hindered Efforts on Terror," *New York Times*, October 7, 2001, p. A1; see also Dan Eggen, "Moussaoui Probe Pushed U.S. Limits," *Washington Post*, January 31, 2002, p. A1.

[30] See CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview fo the Statutory Framework and Recent Judicial Decisions* by Elizabeth B. Bazan, and CRS Report RS21472, *Proposed Change to the Foreign Intelligence Surveillance Act (FISA) under S.113* by Jennifer Elsea.

[31] See CRS Report RS21283, *Homeland Security: Intelligence Support*, by Richard A. Best, Jr., updated May 14, 2003.

Department officials who believed that pressing the Saudis would complicate efforts to work with Riydah on other important issues.[32]

The relationship of intelligence collection to law enforcement in dealing with terrorism poses complex issues for policymakers. Terrorism can, of course, be attacked militarily without concern for domestic law enforcement, but most observers believe that such an approach is appropriate and practical only when terrorists directly threaten the U.S. homeland. In other cases, law enforcement may be the approach that can effectively deal with the problem while not undermining support for larger policy interests or leading to significant U.S. casualties.

Information used in judicial proceedings is often of a different type than that usually collected by intelligence agencies.[33] It is collected differently, stored differently, and must usually be shared to some extent with opposing attorneys. Nevertheless, over the past decade a series of initiatives have been undertaken to enhance the usefulness of information collected by intelligence agencies to law enforcement agencies and vice versa.[34] The barriers to flow of information between the two communities were both administrative and statutory. Both types have been addressed by executive branch policies[35] and by the passage of the USA-Patriot Act of 2001 (P.L. 107-56) which specifically lays the groundwork for making information collected by law enforcement agencies, including grand jury testimony, available to intelligence agencies.

Bringing law enforcement and intelligence closer together is not without challenges. First, the two sets of agencies have long-established roles and missions that are separate and based on constitutional and statutory principles. The danger of using intelligence methods as a routine law-enforcement tool is matched by the danger of regularly using law enforcement agencies as instruments of foreign policy. Bureaucratic overlap and conflicting roles and missions are not unknown in many governmental organizations, but such duplication is viewed with great concern when it affects agencies with power to arrest and charge individuals or to affect the security of the country. Congress may explore the ramifications of bringing the two communities closer together.

Most observers believe that, even if statutes and policies encourage closer cooperation between intelligence and law enforcement agencies, there will many

---

[32] See Elsa Walsh, "Louis Freeh's Last Case," *New Yorker*, May 14, 2001, p.76. Former National Security Adviser Samuel Berger responded to this perception, *New Yorker*, July 2, 2001, p. 5.

[33] See CRS Report 95-1204, *Intelligence Agencies' Information Support to Law Enforcement*, and CRS Report RL30252, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, by Richard A. Best, Jr.

[34] Recently, there have been media reports that the Defense Department's major regional commanders have requested that the FBI and Treasury Department assign representatives to their staffs to help speed interrogation of suspected terrorists and coordinate efforts to freeze bank accounts. See Eric Schmitt, "4 Commanders Seek Staff Role for the F.B.I." *New York Times*, November 20, 2001.

[35] See *Intelligence and Law Enforcement*.

bureaucratic obstacles to be overcome. Within the Intelligence Community there has been a tendency to retain information within agencies or to establish special compartments to restrict dissemination for security reasons. Similar tendencies exist among law enforcement agencies that guard information necessary for their particular prosecutions. Some observers suggest that channels for transferring information must be clearly established and that close encouragement and oversight by both the executive branch and congressional committees would be required to ensure a smooth functioning of transfer arrangements.

A key issue is the overall direction of the effort. As has been noted, the only person with responsibility for the direction of both intelligence and law enforcement efforts is the President. The Bush Administration, like its recent predecessors, has instituted arrangements by which the Justice Department is included in the deliberations of the National Security Council (NSC).[36] There are few complaints that such arrangements do not work effectively at present, but there were situations during the Clinton Administration when it was believed that FBI Director Louis Freeh did not share important information with the NSC and the White House.[37] Law enforcement may require that some information be closely held and not shared outside the Justice Department, but if law enforcement and intelligence efforts are to work more closely in dealing with international terrorist threats, procedures will have to be in place to ensure that important information is shared. Such arrangements would arguably require close monitoring by the President himself, but that could prove a burden upon his time.

A significant issue for Congress is how to budget and conduct oversight of intelligence and law enforcement efforts engaged in counterterrorist efforts. The fact that intelligence and law enforcement agencies are in separate functional categories for budgeting purposes has contributed, in the view of some observers, to different resource environments and indirectly to the acquisition of incompatible information technologies. In general, they argue that for many years the budgets of law enforcement agencies have faced significantly tighter constraints than have those of intelligence agencies. In particular, sophisticated information technology (IT) systems have been acquired by intelligence agencies that, while expensive, have absorbed only a small percentage of annual national defense spending. Acquisition of the similar levels of IT capabilities by the FBI and other law enforcement agencies was not feasible since much higher percentages of administration of justice spending would have been needed. Hence a seamless system encompassing all echelons of intelligence and law enforcement agencies for storing and exchanging information in real time on potential terrorist threats has yet to be developed.

Observers believe that any effort to enhance intelligence and law enforcement IT resources across agencies boundaries will require a determination by both the

---

[36] See CRS Report RL30840, *The National Security Council: An Organizational Assessment*, by Richard A. Best, Jr.

[37] See Walsh, "Louis Freeh's Last Case," pp. 72-73. Other reports suggest, perhaps in retaliation, that Freeh was not given advance notice of the August 1998 missile attack on the Al Shifa pharmaceutical plant in Khartoum. See Seymour M. Hersh, "The Missiles of August," *New Yorker*, October 12, 1998, p. 35.

executive and legislative branches since the budgeting process is a shared responsibility. The Office of Management and Budget (OMB) forwards to Congress each year a proposed budget broken down into functional categories with most intelligence agencies falling into the National Defense (050) category and the FBI and other law enforcement agencies being in the Administration of Justice (750) category. When Congress passes the annual budget resolution, funding levels for the various functional categories are allocated to separate Appropriations sub-committees (in a process known as the 302(b) allocations). This process can create procedural hurdles to the shifting of funds from one functional category to another. Therefore, both branches may review the need to make a coordinated inter-agency examination of law enforcement and intelligence spending on counterterrorism.[38]

Intelligence agencies are overseen by the two select intelligence committees, the appropriations committees, the armed services committees, and others that monitor intelligence efforts of various Cabinet departments. Most observers believe that the Intelligence Community receives reasonably thorough oversight even if comparatively little is shared with the public. Intelligence committees are widely perceived as taking a bipartisan approach to oversight. Despite a widely-perceived need for greater centralized coordination of the Community, the fact that most of the nation's intelligence effort is undertaken in the Defense Department complicates oversight. Law enforcement agencies receive oversight from the two judiciary committees and the appropriators, but observers point out that the primary oversight of law enforcement agencies is provided by the courts in which success or failure is ultimately judged. Judiciary committees have often reflected strong differences over legal issues and nominations. As a result, the nature and extent of congressional oversight for intelligence and law enforcement agencies are different.

Nevertheless, some observers believe that, given the scope of law enforcement involvement in the counterterrorism effort, there may be a need for greater congressional scrutiny of the overall intelligence-law enforcement relationship. The emphasis on homeland defense issues may lead some to call for different forms of congressional oversight.

Intelligence Support to Counterterrorist Military Operations

The campaign against Afghan-based terrorists and the Iraq war of 2003 (which was characterized as related to the war on terrorism) graphically demonstrated the importance of changes in intelligence support to military operations since the end of the Cold War. Beginning with Desert Storm in 1991, U.S. military operations have increasingly depended on precision guided munitions (PGMs) to hit targets while minimizing losses of civilian lives. Precision attacks in turn depend upon accurate and precise intelligence. Some of this data is acquired by humint — especially

---

[38] Section 311 of the Intelligence Authorization Act for FY2003 (P.L. 107-306) established a requirement that cross-agency budget aggregates for total expenditures (in the National Foreign Intelligence Program) for counterterroism be indicated in budget submissions (along with totals for counterproliferation, counternarcotics, and counterintelligence).

important in identifying structures in which key terrorist leaders may be located. Much also derives from imagery collected overhead by unmanned aerial vehicles (UAVs), manned aircraft, and satellites. Other information derives from the signals intelligence (sigint) effort. These new operational concepts, part of the larger effort to transform the nation's defense strategy and force structure, have proven useful in operations conducted against terrorist organizations where the focus is on attacking small groups or facilities and avoiding wide-scale strikes on population centers.

The growing dependence of U.S. military forces on precise and real-time intelligence support requires a significant investment by the Intelligence Community as well as new organizational arrangements. Although satellite imagery is undoubtedly useful, especially in locating fixed installations, much of the tactical intelligence used in military campaigns against terrorist units is provided by manned aircraft such as the U-2s and UAVs such as the Predator and the long-range, high altitude Global Hawk. The linkage of such platforms to platforms armed with PGMs contributed significantly to Allied success in the Persian Gulf War of 1991 and to Operation Allied Force in Kosovo in 1999.[39] The Iraq War of 2003 and the Afghan campaign of 2001-2002 have once again graphically demonstrated their value in operations against terrorist targets.

Although the value of such intelligence collection platforms is almost universally recognized, the numbers available to DOD are limited.[40] As recently as mid-2000 DOD was considering decommissioning U-2s in order to make additional funding available for future Global Hawk procurement.[41] Secretary of Defense Donald Rumsfeld noted in his National Defense University speech on January 31, 2002, "the experience in Afghanistan showed the effectiveness of unmanned aircraft — but it also revealed how few of them we have and what their weaknesses are." He stated that the Defense Department plans to add "more of what in the Pentagon are called 'Low Density/High Demand' assets — a euphemism, in plain English, for 'our priorities were wrong and we didn't buy enough of the things we now find we need.'" FY2004 defense authorization legislation is expected to include significantly increased amounts for UAVs and other platforms.

A recurring problem in tying together the sensors with the attack platforms has been the communications links. Major compatibility problems in Desert Storm

---

[39] See CRS Report RL30366, *Kosovo: Implications for Military Intelligence*, by Richard A. Best, Jr. General Wesley Clark, the NATO Commander during Kosovo operations recalled, however, that, "In Kosovo my commanders and I found that we lacked the detailed prompt information to campaign effectively against the Serb ground forces. Most of the technologies we had been promoting since the Gulf War were still immature, unable to deal adequately with the vagaries of weather, vegetation, and urban areas, or the limitations of bandwidth and airspace. The discrete service programs didn't always fit together technically." *Waging Modern War* (New York: Public Affairs, 2001), p.459.

[40] See CRS Report RL31872, *Unmanned Aerial Vehicles: Background and Issues for Congress*, by Elizabeth Bone and Christopher Bolkcom, April 25, 2003.

[41] See CRS Report RL30727, *Airborne Intelligence, Surveillance and Reconnaissance (ISR): the U-2 Aircraft and Global Hawk UAV Programs*, by Christopher Bolkcom and Richard A. Best, Jr.

meant that some computer printouts had to be sent by air to various commands in the area. Many of the problems were corrected by the time of Kosovo operations and information flowed freely in the theater and back and forth to U.S. agencies in real-time. Media reports have not reflected such communications problems in either Afghan operations or the Iraq War.

The integration of intelligence analysis directly into military operations requires adjustments to organizational relationships among intelligence agencies. Imagery and sigint usually undergo some degree of analysis before the product can be used. Target identification can require input from a variety of intelligence disciplines and in some cases must be approved by Washington-level agencies. Enabling agencies in Washington and elsewhere to support low-level combat units (on a 24-hour basis) involves a high degree of responsiveness and flexibility. Such support may, in addition, come at the cost of other responsibilities. Some observers express concern that support to military operations, including counterterrorist operations, may detract from traditional, but still important missions of providing continuing strategic and geopolitical analyses for national policymaking.

Congress has acknowledged the need for better displays of data, tied to geographical reference points, on computer links that would be available to all military echelons and civilian policymakers. The displays would incorporate information from all intelligence disciplines, including humint and open source materials and would be made available in real-time. The issue for Congress is the extent to which the National Imagery and Mapping Agency (NIMA), a relatively young agency, should have the primary responsibility for maintaining a global system intended to be used throughout the Defense Department and Intelligence Community.

The U.S. military services are in a period of transformation that will pose many issues for Congress.[42] Requirements for capabilities to ensure information dominance and for large numbers of precision weapons will be reviewed alongside programs to replace aging platforms. Ensuring that data collected from a myriad of sensors is available within essential time constraints will require coordination of programs some of which are managed by DOD and others by CIA. The programs are overseen by intelligence and armed services committees. The coordinative process has been imperfect in the past and observers believe that it will continue to be difficult to ensure that weapons platforms and intelligence systems work together effectively. Ties between intelligence and armed services committees are historically close, but observers may suggest new oversight structures.

---

[42] For further background on the transformation process, see CRS Report RS20851, *Naval Transformation: Background and Issues for Congress*, by Ronald O'Rourke; CRS Report RS20859, *Air Force Transformation: Background and Issues for Congress*, by Christopher Bolkcom; and CRS Report RS20787, *Army Transformation and Modernization: Overview and Issues for Congress*, by Edward Bruner.

Conclusion

Effective counterterrorism — political, diplomatic, and military — requires good intelligence, but counterterrorism intelligence differs in many ways from the intelligence support that was needed during the Cold War and for which the Intelligence Community remains in large measure organized. Significant challenges lie in the area of humint collection where practices that might produce much valuable information could be expensive and involve the United States in activities that, if revealed, could be highly controversial at home and abroad.

Intelligence and law enforcement are becoming increasingly intertwined. Few doubt that valuable insights can derive from close correlation of information from differing intelligence and law enforcement sources. Should the two communities draw too close together, however, there are well-founded concerns that either the U.S. law enforcement effort would become increasingly inclined to incorporate intelligence sources and methods to the detriment of long-standing legal principles and constitutional rights or, alternately, that intelligence gathering in this country or abroad would increasingly be hamstrung by regulations and procedural requirements to the detriment of the national security. Difficult decisions will have to be made (some affecting organizational responsibilities), and fine lines will have to drawn.

Observers believe that the campaign to counter terrorism will tend to reinforce the perceived need to transform the U.S. defense structure to take full advantage of information technologies and precision munitions. Counterterrorist missions may not dictate the procurement of platforms, but they are likely to have an important influence on the intelligence collection, communications, and information links.

At the same time, observers caution that the current war on terrorism which has accentuated the need for law enforcement and intelligence cooperation may not, despite Administration projections, be a decades-long endeavor. They argue that even as Al Qaeda and other terrorist organizations are being dealt with, traditional geopolitical concerns remain. Given the nature of organizational dynamics, they suggest, it may be difficult to maintain adequate expertise on international military and geopolitical issues that will remain of vital concern in the future. Terrorist threats have become a central concern for the U.S. Intelligence Community, but the rest of the world has not disappeared from policymakers' horizons. As Secretary of Defense Rumsfeld stated in his National Defense University speech, "we cannot and must not make the mistake, of assuming that terrorism is the only threat. The next threat we face may indeed be against terrorists — but it could also be a cyber-war, a traditional, state-on-state war... or something entirely different."