ATTACKING TERRORISM

Elements of a Grand Strategy

Audrey Kurth Cronin and
James M. Ludes, Editors

In cooperation with the
Center for Peace and Security Studies
Edmund A. Walsh School of Foreign Service
Georgetown University

Georgetown University Press

five

INTELLIGENCE

Paul R. Pillar

The basic problem that terrorism poses for intelligence is as simple as it is chilling. A group of conspirators conceives a plot. Only the few conspirators know of their intentions, although they may get help from others. They mention nothing about their plot to anyone they cannot absolutely trust. They communicate nothing about their plans in a form that can be intercepted. They are careful not to expose to others any materials that would betray their intentions. They do not purchase, procure, or build anything that, on the face of it, is suspicious. They live and move normally and inconspicuously, and any preparations that cannot be done behind closed doors they do as part of those movements. The problem: How do we learn of the plot?

The challenge does not stop there. As with many perpetrators of past terrorist attacks, the conspirators whose plans we need to discover may not have had any prior involvement in terrorism or be members of a previously known terrorist group. The target for intelligence is not just proven terrorists; it is anyone who *might* commit terrorism in the future.

Terrorism is a fundamentally different and more difficult subject than the great majority of other topics the intelligence community is asked to cover. The bull's-eye of this intelligence target—an individual terrorist plot—lacks the size and signatures of most other targets, from nuclear weapons programs to political instability. The need to uncover the activities not only of specified groups or states but also of *potential* terrorists makes intelligence ques-

tions about terrorism, not just the answers, more indeterminate than with most other topics. Some of the most important limits to collecting information about terrorism are inherent to the subject and the way terrorists operate. Those limits are permanent and ineradicable.

A painful but true implication is that no matter how much brainpower and resources the United States devotes to counterterrorist intelligence, how much brilliance goes into the relevant intelligence operations, and how aggressively the intelligence community is reorganized or revamped to go after the problem of terrorism, some of what terrorists do will remain, for all practical purposes, unknowable. Some terrorist plots will go undiscovered, and some terrorist attacks, including some major ones, will occur. Intelligence has an enormously important role in learning as much as can be learned about terrorists' activities and in so doing reducing the number of terrorist incidents and lives lost. U.S. intelligence has saved lives from terrorism in the past, and how well it performs its mission will be a major determinant of how many American lives will be lost to, or saved from, terrorism in the years ahead. But even the best intelligence will never be able to save them all.

In this chapter I describe the functions that intelligence performs in counterterrorism, as well as what it should *not* be relied upon to do; the directions in which the U.S. counterterrorist intelligence apparatus has already evolved; and the aspects in which future change and evolution hold the most promise of improving (but only modestly) the results. I conclude with a caution about how some well-intentioned attempts to get U.S. intelligence to do even better on terrorism can be counterproductive. I argue for care and restraint in making changes—particularly in the emotional aftermath of wrenching terrorist attacks, which is when most changes to counterterrorist programs are made—and for realism in expectations about the part intelligence can play in helping to safeguard a nation against terrorism.

Functions of Counterterrorist Intelligence

The counterterrorist role that intelligence most commonly is expected to perform is to discover the details of terrorist plots so that the plots can be rolled up before they are carried out or, as a second-best response, the intended targets can be protected by relocating them, augmenting security, or canceling or rescheduling events. This is the most direct, most satisfying, and—when such incidents are made public—the most spectacularly successful way in which intelligence can help to curb terrorism. Certainly intelligence agencies need to do what they can to increase their odds of collecting this kind of plot-specific intelligence. For the reasons mentioned above, however, intelligence specific to terrorist plots often is unattainable. This function, how-

ever satisfying and potentially spectacular, therefore will never be the biggest contribution that intelligence makes to counterterrorism.

That truth is uncomfortable not only for the public but for security managers. Given the costs—monetary and nonmonetary—of security countermeasures and preventive actions such as closing an embassy or canceling a flight, there is an understandable tendency to rely on tactical warning so that protective measures can be bolstered when threats are present but relaxed when they are not. As the panel led by retired Admiral William Crowe that studied the bombings of the U.S. embassies in East Africa in 1998 noted, that tendency is a mistake.[1] It puts too much faith in the likelihood of collecting tactical intelligence on whatever will be the next terrorist plot to materialize. Intelligence agencies must work to dispel that misplaced faith. They have a responsibility not only to report to their consumers what useful information they have but also to instruct them on the limits of the intelligence they are providing, including some sense of what is *not* known. There is no subject on which that responsibility is more important than the warning of terrorist attacks.

The largest contribution that intelligence actually makes to counterterrorism is the collection of information on individual terrorists, terrorist leaders, cells, and groups that is used to disrupt terrorist organizations. The information collected can be quite specific (names, addresses, phone numbers, etc.), even if it does not identify specific plots. Terrorists are highly security conscious about their attack plans, but they do not live and operate in cocoons. They have identities (albeit sometimes multiple ones), they meet, they move, and they communicate. There are many types of collectable information that, though fragmentary and incomplete, can provide clues to the location, activities, and associations of suspected terrorists. With enough such clues, a would-be terrorist can be arrested, deported, interrogated, or even prosecuted. Cells can be broken up and their members left to wonder what each one may be telling to the authorities.

Although every counterterrorist instrument must be used to the fullest, in some respects the terrorist-by-terrorist, cell-by-cell disruption of terrorist infrastructures is the most fruitful. To be sure, this instrument—like all the others—has considerable limitations. The most serious is the uncertainty that a would-be terrorist, especially one who has not been involved in previous attacks, will come on to the intelligence agencies' screens in the first place. The potential payoffs, however, also are considerable. Put up security countermeasures around one potential terrorist target and you have protected that one target from attack (probably attack through one particular method), for as long as you keep the security in place. Disrupt a terrorist cell and you have prevented that cell from attacking any target, at any time, with any method. Because terrorists often commit other illegal acts (such as smuggling or use

of false documents), disruption of their organizations can build on the enforcement of national laws by foreign police and security services. There also are beneficial secondary effects. Disruption can sow suspicion and distrust within a terrorist organization far beyond the cell that is disrupted, and materials that are confiscated when a cell is broken up often provide intelligence leading to the disruption of other cells—even cells in other countries. Most of the counterterrorist successes by U.S. intelligence have involved such disruption.

Intelligence makes many different types of analytic contributions to counterterrorism. Even the contributions that can be described as warning or assessment of terrorist threats cover a broad range, from the highly tactical to the broadly strategic (see table 5–1). These contributions, in turn, serve a comparably broad range of ways in which the nation tries to meet the threats. Toward the tactical end is the task of sifting through the snips and shards of information about possible terrorists and suspected terrorist cells, trying to make enough sense of it to distinguish terrorists from nonterrorists, to cause possible disruption of terrorist cells, and to guide the collection of further intelligence that would fill knowledge gaps. At a less tactical level there are a host of analytic questions such as questions concerning the intentions and capabilities of large terrorist organizations or the overall terrorist threat in a given country or region. Intelligence analysis at this level has saved lives; for example, the assessment that the terrorist threat to U.S. forces in Saudi Arabia was high at the time of the bombing at Khobar Towers in 1996 underlay security measures that prevented the truck carrying the huge bomb from penetrating the perimeter of the military compound. Penetration would have produced a death toll far higher than the nineteen servicemen who did die. At the most strategic level, analysis becomes a task of educating the consumer of intelligence on global trends and patterns in international terrorism. The policy decisions informed by this kind of analysis include overarching decisions involving the resources devoted to counterterrorism and how counterterrorism should fit in the larger foreign policy agenda.

Intelligence supports other counterterrorist instruments in many ways that go beyond warning or assessment of terrorist threats. Intelligence about the nature and activities of extremist groups provides the basis, for example, for decisions on designating foreign terrorist organizations (FTOs) under U.S. law. Intelligence makes a similar contribution regarding the activities of state sponsors of terrorism. It supports diplomacy not only by informing senior officials who have to make designation decisions and persuade other governments to cooperate in counterterrorism but also in developing material that can be shared with those governments. When military force is used in a counterterrorist mode, the contribution of intelligence includes the determi-

Table 5-1 Spectrum of Terrorism Warning and Threat Assessment

Types of Threat Information		Plot-Specific	Tactical	Strategic	Grand Strategic	Educational
Specificity of information	Location	Exact address	A few cities	Country or region	Regions	Worldwide
	Time	Exact date	Days or weeks	Weeks or months	Months or years	Years or decades
	Targets	Single named target	Several named targets	Single category of interests (e.g., embassies or military bases)	Several categories of interests	U.S. interests
Possible countermeasures		Roll up the plot; evacuate or relocate the target	Short-term, high-cost security measures; watch for the perpetrators	Raise alert levels; temporary but sustainable security measures	Permanent new physical measures and procedures	Legislation; major national programs

nation of responsibility for terrorist attacks to which the military action is a response, as well as the same sort of support to military targeting that is provided whenever armed forces are used for other purposes. Support to law enforcement includes detailed exchanges of information and following up on leads, not just to determine responsibility for terrorist crimes but to chase down the perpetrators.

Intelligence analysis on terrorism is all-source analysis. That is, it draws on every available source of information—human and technical intelligence sources, as well as what is publicly available—to develop insights about terrorist activity. Much of the analysis parallels analytical work outside government, but the intelligence analyst is the only one who can meld the classified information with the unclassified and guide the efforts of intelligence collectors to attempt to fill in the gaps.

Counterterrorist intelligence analysis includes a couple of other functions that, though valid, are—like the collection of plot-specific tactical intelligence—not as large a part of the job of intelligence as is often supposed. One is the prediction of terrorist tactics and techniques (which is related to the issue of targets). Among the frequent reactions to a terrorist attack is the posing of the question, "Why didn't someone think of that method of hitting us?" The answer usually is that the tactic was indeed considered—but so were dozens of other possible methods that terrorists could use, many of which were equally plausible. Intelligence reporting sometimes reveals that certain groups are interested in a particular method of attack or even devel-

oping the capability to use that method. Intelligence analysis must use that reporting in sensitizing security managers and policymakers to the range of terrorist tactics they should be prepared to counter and in explaining why terrorists may be turning more to some tactics than to others. Intelligence agencies have no special advantage, however, in blue-sky speculation about methods terrorists might use in the future. Thinkers outside government do plenty of that kind of speculation. Whether inside or outside government, predicting the specific method to be used in the next major terrorist attack gets back to the basic problem of trying to uncover plot-specific information. (Before the attacks on September 11, 2001, there was much speculation about ways in which terrorists could hit the U.S. homeland. Most of that speculation involved biological, nuclear, or other exotic materials or methods—musing that may yet turn out to be useful in anticipating future attacks but was irrelevant to the hijackings that did occur.)[2] An agency (or individual analyst) that boldly and correctly predicted the method of the next terrorist attack might be applauded after the fact for prescience, but that prediction probably would be nothing more than a lucky guess.

Another function that is prominent in public perceptions of intelligence analysis is that of "connecting the dots" of information about a terrorist plot in the making. This function is the analytical equivalent of the task of collecting plot-specific information. As with that task, intelligence agencies (usually working in concert with law enforcement) must continually search for all possible connections among whatever fragments of information they have. This function is at the heart of the tactical-level analytical work that intelligence agencies do continually, through techniques such as cross-checking of names and other information with previous reporting and tasking intelligence assets to fill in gaps that may involve still other connections. The reality that the agencies face—and often is overlooked in the aftermath of a major terrorist incident, when there is an understandable focus on the bits of information that pertained to that one incident—is that there is never just one set of "dots" but many of them, each of which can be connected in multiple ways. All of them must be vigorously pursued through all of the name-checking, asset-tasking techniques that are available. Successful pursuit usually results in a disruption—which is likely to prevent future, still-unknown terrorist attacks—rather than the rolling up of a plot in progress. There seldom is a basis for pointing to any one set of "dots" as predictive of the next terrorist attack and worthy of more attention than all the other sets.

Intelligence analysis on terrorism illustrates a principle that is applicable to intelligence analysis generally: It is a business not primarily of prediction but of helping the consumers of intelligence deal with an unpredictable world.[3] It involves enlightening the policymaker about the range of threats, the directions threatening developments may take, the relative likelihood of

each direction, the indicators suggesting that one direction is being taken rather than others, and the implications for the nation's interests of each of the possibilities. In one sense analysis of counterterrorism is even farther removed from prediction than is analysis of other national security issues because the whole purpose of "predicting" a terrorist event would be to prevent it. Counterterrorist analysts could never get as much satisfaction as their intelligence colleagues covering other topics from seeing their predictions come true. A world in which intelligence never "failed" to foresee a terrorist attack would be a world in which there was no longer any terrorism. One prediction that can be made with confidence is that such a world will never materialize.

Evolution of Counterterrorist Intelligence

Amid the rhetoric about how September 11 and the U.S. response to it marked a sea change from an earlier world, the continuity and history of U.S. efforts against terrorism get overlooked. The intelligence portion of that effort has received close attention for more than a decade and a half. The methods and institutions that perform the counterterrorist intelligence mission today are the product of evolution throughout that period, with many lessons applied and innovations tried.

Americans first became highly concerned about international terrorism in the 1980s, with buildings bombed and hostages taken in Lebanon and a spate of airplane hijackings elsewhere. (Until September 2001, the deadliest terrorist attack against Americans had been the bombing of the Marine barracks in Beirut in 1983.) The report in 1985 of a task force headed by then-Vice President George H. W. Bush led, in part, to creation the following year of the Directorate of Central Intelligence (DCI) Counterterrorist Center (CTC), which pulled together and augmented counterterrorist work that previously had been performed in different parts of the Central Intelligence Agency (CIA) and the intelligence community. The establishment of the CTC was a bureaucratic revolution, cutting across established hierarchies in the CIA to create an integrated element unlike anything that had come before. The novel aspect of the center was to bring operations officers, analysts, reports officers, technical experts, and other specialists into a single organization. It provided one-stop shopping on everything related to terrorism. It maximized synergy by having members of these different disciplines working literally side by side. The CTC became a model for centers later established to work on subjects such as narcotics and counterintelligence.

Subsequent refinements enhanced the synergy as well as the expertise of the CTC. A permanent professional corps of counterterrorist analysts was

established in the mid-1990s, for example, replacing an earlier system in which analytical resources had to be borrowed from other offices in CIA. Particular emphasis was placed on developing the multiagency character of the center. More than a dozen agencies—including agencies with intelligence, law enforcement, and regulatory responsibilities—came to have full-time representation in the CTC. Sharing and cross-checking of data became easier when, for example, an officer of the Immigration and Naturalization Service (INS) was just a few desks away from a CIA analyst working on a case that involved someone entering the United States. The critical relationship between intelligence and law enforcement received special emphasis, particularly through cross-assignments of personnel. These cross-assignments included a deputy chief's job in the CTC being reserved for a senior Federal Bureau of Investigation (FBI) officer, with a CIA officer of comparable rank filling a corresponding position at the FBI. Such arrangements proved valuable not only in facilitating the flow of information but in breaking down what had been significant cultural barriers between the intelligence and law enforcement portions of the U.S. counterterrorist apparatus.

The intense commitment and imaginative organizational arrangements embodied in the CTC were applied in an even more concentrated way to special topics such as the threat posed by Osama bin Laden. In the mid-1990s, well before bin Laden became a recognized name in the United States or had been placed under indictment and well before anyone had heard of al-Qaeda, the CTC created a special unit focused solely on bin Laden. Resources were shifted into a coordinated effort to learn everything possible about bin Laden and his activities, to develop additional sources of information about him, and to formulate options for policymakers to deal with the threat he posed. Procedures for communicating between headquarters and the field were streamlined to assure quick responsiveness. The unit became a prototype for dealing in a well-focused way with vexing but high-priority problems.

The concentrated intelligence work on bin Laden provided the depth of understanding that became apparent in the wake of later incidents. This work enabled culpability for the bombings of embassies in 1998 to be determined so swiftly and certainly that the president could order a retaliatory strike in a matter of days. It also enabled CIA Director George Tenet to say with high confidence in the first hour after the attack on September 11, without any claims of responsibility and before any postincident reporting, "This has bin Laden all over it."[4]

The development of the CTC took place within a larger context of increasing priority and focus that the intelligence community devoted to counterterrorism. After sharing in general cuts to national security programs in the first half of the 1990s, the CTC and other counterterrorist-related efforts

in the intelligence community were given higher priority in mid-decade after incidents such as the bombing at Khobar Towers raised concerns about terrorism; the priority was raised even further when the embassies in Africa were attacked in 1998. Since at least as far back as the embassy bombings, no subject has received higher priority from the intelligence community than counterterrorism—especially efforts to develop well-placed sources with a chance of obtaining information about plans for future terrorist attacks.

The point of this history is that most of the roads worth trying in counterterrorist intelligence have already been tried. Most of what needed to be reorganized has been reorganized, most of the institutional barriers that needed to come down have been smashed, most of the needed reprioritization has already been done, and most of the fires that needed to be lit under bureaucracies to keep them energized have been burning for some time. The distance the intelligence community has come in improving its counterterrorist efforts is reflected in its considerable successes in the form of terrorist operations preempted, terrorist infrastructures disrupted, and individual terrorists captured and brought to justice. Unfortunately, the intelligence officer's curse of being unable to reveal most of his successes while his failures become public applies in spades to counterterrorism, where the failures are dramatic and traumatic and most of the operations that underlie the successes are especially perishable were they to become known. What the Director of Central Intelligence (DCI) has been able to say publicly about the successes only scratches the surface.[5]

Any posture that smacks of "business as usual," however, will not be tolerated, particularly in the post–September 11 climate. Any answer that sounds like "we were already doing all that could reasonably be done" does not fly before a Congress and a public that want change. There will be continued pressure for new procedures, new organizations, new *something*. Finding things that look new and actually have a chance of improving counterterrorist intelligence will be difficult.

Responding to National Trauma

Significant events that are perceived as intelligence failures invariably are followed by voluminous commentary, as well as statements by congressmen and other quotable figures, on the theme that the U.S. intelligence community has deep flaws and needs overhauling. This phenomenon is especially true of major terrorist incidents. Because of the enormity of the death toll, the aftermath of the attacks on September 11 became the best example. The House Intelligence Committee expressed the prevailing tone in its report accompa-

nying the next intelligence authorization bill by stating that "there is a fundamental need for both a cultural revolution within the intelligence community as well as significant structural changes."[6]

This urge to overhaul is a natural response to the pain of the moment and to the desire to believe that by changing things we can somehow avoid a recurrence of the pain. The unfortunate irony is that these moments when there is the greatest political support for change in some respects are the least favorable times for enacting sound, well-thought-out changes. The sheer emotion and atmosphere of recrimination do not lend themselves to well-reasoned debate. There usually is rush to legislate, with anniversary dates in mind as arbitrary deadlines (true of the omnibus counterterrorist legislation hurriedly passed in 1996 as the one-year anniversary of the Oklahoma City bombing approached and of debate on the homeland security bill in 2002 before the September 11 anniversary). Application of hindsight to a terrorist event that has just taken place distorts the realities that faced intelligence agencies before the event, with a blurring in the public consciousness of what was known before the incident with what was discovered afterward.

The greatest perceptual problem about intelligence is the tendency to focus narrowly on whatever errors were committed relevant to the most recent case and to draw larger conclusions about overall performance without placing those data points in any larger context. An example from the September 11 case is the issue of communication between the U.S. intelligence and law enforcement communities. A couple of well-publicized mistakes (the CIA's tardiness in placing two of the hijackers on a watch list and resistance by FBI headquarters to letting an FBI field office check some names with the CIA) became the basis for a widely accepted belief—repeated unquestioningly by scores of commentators—that "the FBI and CIA don't communicate with each other." The errors were a tiny fraction of what has been, since increased integration in the mid-1990s, a huge daily flow of terrorist-related leads and other information between those two agencies, as well as between the larger law enforcement and intelligence communities. To base conclusions about what needs to be changed on the publicized errors would be akin to a blind man diagnosing the ailments of an elephant based on a wart he is feeling on one of the animal's legs.

Similar narrowness characterized some other aspects of what came to be accepted wisdom about the U.S. intelligence community's performance relative to September 11. The shock of that event made it easy to overlook how similar the intelligence realities of that case had been to earlier ones—*viz.*, an absence of plot-specific tactical intelligence in the face of plotters who kept their plot well hidden, amid good strategic intelligence about the threat a group was posing to U.S. interests. The September 11 hijackers appear to have taken simple but effective steps, as in the prototypical terrorist plot de-

scribed at the beginning of this chapter, to keep their plans under wraps. They do not appear to have communicated the existence of their plan, let alone the details of it, to anyone beyond a small circle of knowledgeability. Osama bin Laden, in the most revealing of his videotapes, said that even some of the hijackers were unaware of the nature of the operation.[7] Probably only the operation's ringleader, Mohammed Atta; a few of the other pilot/hijackers; and bin Laden and a handful of his lieutenants knew what was going to happen. It is difficult to refute President Bush's contention that the attack was not preventable or the conclusion reportedly reached by members of the Congressional intelligence committees investigating the disaster that there was no single piece of information that, if properly analyzed, could have prevented it.[8]

The strategic intelligence on the terrorist threat that al-Qaeda posed to the United States as September 2001 approached was strong. Director of Central Intelligence George Tenet, in his annual testimony to Congress in February 2001 on worldwide threats to U.S. national security, highlighted the threat from terrorism as "real" and "immediate." He spoke of terrorists as having become more operationally adept, seeking ways to deal with increased security around government and military facilities, and using strategies such as simultaneous attacks to increase the number of people they kill. "Osama bin Laden and his global network of lieutenants and associates," Tenet stated, were "the most immediate and serious threat."[9] These statements were the general warnings in unclassified testimony; as always, the classified intelligence provided to policymakers was more specific. Information collected as the year wore on led the intelligence community to conclude that the threat was becoming even more immediate and serious. Tenet was described as "nearly frantic" during the summer with concern over this threat, and he repeatedly conveyed his warnings to senior administration officials.[10] This was not the face of an intelligence community that failed to recognize a danger. It was a community that recognized the danger clearly, was exploiting every opportunity to collect further information on it, and felt first-hand the frustration of being unable to collect the details of exactly what, when, and where the next attack would be.

Good strategic intelligence with a lack of tactical intelligence has been a recurrent theme in postmortem examinations of major anti-U.S. terrorist incidents. It was a finding of the inquiry led by General Wayne Downing into the bombing of Khobar Towers in 1996.[11] It was a finding of the Crowe panel that examined the bombings of the embassies in Africa in 1998.[12] The theme recurs not because different cohorts of intelligence officers keep making the same mistake and not because of some systemic flaw that the intelligence community stubbornly refuses to correct. It recurs because of the intrinsic difficulty of cracking into the plans of terrorist groups and because of the

type of intelligence that earnest and comprehensive efforts to cover terrorism tend to yield.

Proper understanding of past tragedies is important not to determine whose heads should roll or whose professional pride should be wounded but for two more basic reasons having to do with how intelligence efforts against future terrorism ought to be designed and organized. One reason is that fixing something requires a clear understanding of what is—or is not—broken. Change for the sake of change may help a losing baseball team, say, but it is unlikely to save lives from future terrorism.

Another reason is to understand how much of a contribution intelligence can and should make to the overall counterterrorist effort. Getting plot-specific tactical information clearly is an intelligence responsibility; it is hard to imagine any "policy failure" at that level because the obvious response to getting such information is to roll up the plot. At the more general level where most of the available information exists, however, the intelligence community often can only lead the policy horse to water but not force it to drink.

An example is the employment of military force in Afghanistan. The United States used arms in the autumn of 2001 to sweep away al-Qaeda's headquarters, its training camps, and the regime that hosted them because the attack on September 11, like the Japanese attack on Pearl Harbor, so enraged the American public and government that they were willing to assume costs and risks they would have shunned in the absence of such a calamity. Unlike Pearl Harbor (before which there might have been doubt about Japan's intention to make war against the United States), however, September 11 revealed nothing new about the intentions or general capabilities of al-Qaeda. The size and scope of the group's presence in Afghanistan, its relationship with the Taliban, its global reach, and most of all its intention to do the United States deadly harm were the subjects of repeated—and accurate—production by the intelligence community. Military intervention in Afghanistan did not extinguish al-Qaeda, and a preemptive attack there would have been harder to justify internationally than the post–September 11 operation that took place. The intelligence community's performance had very little to do with the United States waiting until after the September 11 disaster to finally clean out the terrorist den that Afghanistan had become.[13]

Organizations, Personnel, and Cultures

The dominant themes in discussions of how to improve U.S. intelligence have been sounded for years. They are heard more frequently following major terrorist attacks. Truly new ideas are scarce. Few of the ideas expressed relate specifically to terrorism. Many of them involve valid principles for a sound

intelligence program but do not entail change from what is already being done. Many of them relate less to how the intelligence community actually operates than to lore, passed from commentator to commentator, of how it is presumed to operate. Almost none of them offer a way of cracking the conundrum of penetrating terrorist plots.

How does the intelligence community (or the president, or Congress) respond to entreaties such as to "get more human sources of intelligence on terrorist groups"? There certainly is no substitute for a human source within a group, particularly within the inner circle that does the plotting and planning—which is why the leadership of the intelligence community has placed such high priority on the recruitment of such sources. One has to search hard, however, amid expressions of dissatisfaction with the intelligence community's performance, to find even semispecific ideas about how the community might do things differently.

One subject of potential ideas is the organization and structure of the intelligence community. The decades-old issue of the DCI's control (or lack of it) over the entire community, for example, is receiving renewed attention.[14] That attention is healthy, and the issue is important for other reasons. It is difficult to see, however, how redefinition of the DCI's relationship with intelligence agencies other than the CIA—or other mixing or merging of agencies—would make any discernible difference in the quality of counterterrorist intelligence. The integration already achieved through such mechanisms as the CTC, along with the consensus among all agencies that counterterrorism deserves top priority, makes discussion of, say, where the National Security Agency (NSA) should fit in the government's organization chart seem almost irrelevant.

An organizational change that would make a greater difference for counterterrorism would be to centralize work on the subject even further by merging the counterterrorist functions of the intelligence and law enforcement communities. One proposal would do this by essentially shifting the CTC to the FBI.[15] Although this shift would appeal to the oft-expressed objective of enhancing cooperation between intelligence and law enforcement, it would have the disadvantage of separating the resulting counterterrorist entity from the field elements (necessarily run by the CIA's Directorate of Operations) that collect human intelligence on terrorism. Integration in counterterrorist work is important—which is why so much has been done already—but it already is near the point beyond which further integration would yield little or no improvement. That is the main reason it is important to have a clear understanding of existing cooperation between the intelligence and law enforcement communities.

Another frequent subject of comment is the quality of the intelligence community's personnel. A common refrain is that the community needs to

recruit more bright, talented people to work on counterterrorism. "When I was there, we could not get a single person from the Ivy League to join the CIA," complained one retired (and anonymous) official. "To fight terrorism, we need to deal with the dregs of the Earth, and we need very bright Americans who can figure out how to go overseas and do these things."[16] Recruitment into this segment of public service, like most other segments, no doubt has been affected adversely by the relative attractiveness of career opportunities in the private sector (although the Ivy League has been represented at the CIA all along). The end of the economic boom of the 1990s and a surge in interest in intelligence work following September 11 already may be changing the incentives of potential recruits.[17] Quality of personnel matters, of course, and this particular security need is just one of many reasons to maintain strong incentives for talented people to enter and remain in public service. It would be the hubris of the best and the brightest, however, to think that the problem of penetrating terrorist groups is solvable simply by applying enough smarts to the problem.

A related theme centers on the alleged eclipse of a certain type of CIA specialist: the field operations officer, fluent in the language and steeped in the culture of the country in which he works and collecting critical information through wits, daring, intrigue, and local knowledge. This theme—heard disproportionately from former operations officers—includes the complaint that reward structures have evolved to where "a year in some country where it was dangerous to drink the water would get you no farther up the ladder than a year pushing paper in Langley."[18] The type of officer whose deemphasis is lamented is indeed critical to the collection of intelligence on terrorism—which is why that type has not been deemphasized at all for at least the past five years. To the contrary, a major priority of the CIA and the congressional committees that authorize and appropriate its funds has been the recruitment and training of that type of officer—part of a long-term effort to reverse earlier downsizing of the field operations corps.

Valuable though the individual, unilaterally collected nugget of terrorism intelligence may be, the rarity of true nuggets (because of the inherent difficulty of penetrating terrorist groups) means that most intelligence breakthroughs against terrorism will continue to involve the piecing together of nonnugget-like information from a variety of human, technical, and open sources. Critical contributions to such breakthroughs are made by analysts who do the piecing together, reports officers who get information into the hands of those who can exploit it, and managers who ensure that collection resources are deployed where they will complement rather than duplicate other sources of information. The transnational nature of the terrorism that most threatens U.S. interests accentuates the importance of piecing together disparate information collected in widely separated places. Terrorist opera-

tions that are funded on one continent, planned on another continent, and carried out on a third by perpetrators of multiple nationalities (as was true of the attacks on September 11) are unlikely to reveal their entire shape to even the most skillful local collection effort. Living where the water is bad, by itself, is apt to yield more stomach ailments than insights about terrorism—insights that are at least as likely to be gleaned in the papers being pushed at Langley.

Another theme of discussions of U.S. intelligence concerns institutional culture. Critics of the CIA in particular repeatedly describe it as "risk averse."[19] This label has become such common currency that it gets repeated matter-of-factly by commentators who have no way of knowing whether it is true—and in the face of the few public indicators of the actual level of risk-taking in the agency (such as the fact that the first U.S. death from hostile fire during Operation Enduring Freedom in Afghanistan was a CIA officer, killed while interrogating detainees for terrorist-related information).

The issue of risk aversion has centered around CIA guidelines established in 1995 that required additional senior-level headquarters approval for recruitment of intelligence sources suspected of having committed human rights abuses or other serious acts of violence. The National Commission on Terrorism recommended rescinding the guidelines, which it charged had inhibited recruitment of sources with potentially valuable information on terrorism.[20] The commission's recommendation appeals to the sense that anything that involves more bureaucracy is bad and anything that lets risk-taking officers in the field get on with the job of fighting terrorism is good. "After all," points out one commentary on the subject, "James Bond never had to fill out paperwork or myriad bureaucratic forms."[21] However, the effect, if any, that the guidelines have had on recruitment of sources of intelligence on terrorism has been greatly overstated. Every proposal that has come to headquarters for approval under the guidelines has been approved, with delays too minimal to affect either the success of the recruitment or the usefulness of any information gathered. Moreover, if risk aversion is a problem, having senior management buy into a potentially controversial recruitment before it is made reduces the risk to the individual officer who does the recruiting.

At least the commission's recommendation had the virtue of being specific. Codifying it, however—as Congress attempted to do in the Intelligence Authorization Act of 2002—is more difficult. (How does one tell the head of an agency *not* to exercise supervision intended to ensure respect for human rights?) The result sounds like a buzzword-laden exhortation rather than a law. The legislation instructed the DCI to replace the 1995 guidelines with "new guidelines that more appropriately weigh and incentivize [*sic*] risks to ensure that qualified intelligence officers can and should swiftly gather intelligence from human sources in such a fashion as to ensure the ability to

provide timely information that would allow for indications and warnings of plans and intentions of hostile actions or events, and ensure that such information is shared in a broad and expeditious fashion so that, to the extent possible, actions to protect American lives can be taken."[22] This kind of flourish is of little use as guidance in establishing operational rules and procedures. Nonetheless, the agency has rescinded the 1995 guidelines and has tried to make the human rights considerations underlying them an integral part of the larger headquarters review process that is essential to any human intelligence operation. The process is essential because other information must be applied to direct human collection resources to where they are most needed and likely to be most effective, as well as to assess the credibility and access of agents. It is ironic that much commentary about counterterrorism notes the need to integrate data from different sources but overlooks this aspect of integration in managing the collection of human intelligence.

Reality, Not Romanticism

The image of the Ivy Leaguer who goes where it is dangerous to drink the water and—unencumbered by annoying instructions from headquarters—applies his brilliance and James Bond-like daring to the job of saving America from terrorism appeals to our imaginations but has little to do with the real business of intelligence and counterterrorism. The task ahead for the intelligence community appears more mundane, not only because it lacks the romantic aspect of that image but because it is not all that different from what it has been for some time. Obviously there is room for improvement—as there will be as long as the counterterrorist batting average is not 1.000, which means indefinitely—but even large increases in what U.S. intelligence does, or major changes in how it does it, offer only modest prospects for more reassuring results.[23]

More well-trained operations officers in the field, as well as more analysts and other critical personnel and the monetary and technical resources to go with them, will make a difference, but not in the sense of closing some key and well-defined gap that has kept the United States from going the last mile it needs to go to find out what terrorists are up to. Rather, such increases would marginally heighten the chance of gaining useful information and insights about terrorist activity, which in turn would marginally heighten the chance of forestalling some future terrorist attacks and saving some lives. They would do so by alleviating shortages that—despite the considerable increases in dollars and manpower devoted in recent years to counterterrorism—still limit the ability of several agencies to carry out the sweeping tasks they are now being relied upon to perform. The FBI, for example, simply

does not have the manpower to surveil and investigate everyone in the United States who ought to be scrutinized for possible connections to terrorism.[24] Similarly, there would be less risk of slip-ups or slowness at the CIA or NSA in processing, exploiting, and disseminating information if the typical crushing load of information to be processed could be distributed into more manageable proportions to be handled by more hands. Sound management and adroit use of automation are critical but can go only so far. The core of the work to be done—the part that will be the stuff of inquiries after future major terrorist incidents—will still have to be done by skilled people collecting, assessing, and acting on individual pieces of information.

Beyond the question of resources, there are two principal areas in which to look for potential improvements in intelligence about terrorism. Both go beyond what the intelligence community itself can do. The first concerns the acquisition of information from foreign governments. Probably no other intelligence topic depends more on foreign liaison than does terrorism. Certain foreign governments will always be better able than the United States to operate against certain terrorist groups, for reasons of geography, culture, or past contacts. The willingness of those governments to share intelligence depends not only on what the CIA does to cultivate the liaison relationships but also on the overall state of bilateral relations with the United States, and that is a function of broader U.S. foreign policy. Moreover, some of the governments with the most intelligence to share about terrorists are ones that have presented significant problems, including terrorist-related problems, for U.S. policy. To collect intelligence on terrorism, the United States needs to take risks in dealing with regimes—not just individuals—with blood-stained pasts.

The other area for attention involves the integration of intelligence with nonintelligence sources of information. This does not primarily mean the criminal investigations of law enforcement agencies such as the FBI, where integration with intelligence for counterterrorist purposes already is extensive. The greatest potential opportunities for further integration of information involve other types of data about the movements and activities of large numbers of people—especially data on travel and immigration. Encyclopedic mining of such data for intelligence purposes (as distinct from spot inquiries concerning cases already being investigated) has not been done to date for several reasons, most of which involve the needle-in-haystack aspect of any such endeavor and the prospect that it would yield a meager payoff on a very high investment. A host of practical problems, ranging from the use of pseudonyms by terrorists to the reluctance of some owners of data banks to make them available for such scrutiny, reduces the probable yield further.[25] Moreover, some of the key elements of exploiting information would still have to be done by live analysts assessing *sui generis* cases; they could not be

programmed into a data-mining algorithm. Despite all these limitations, the change since the September 11 attacks in national priorities and in the thresholds for spending resources for counterterrorism warrants fresh attention to this frontier in the exploitation of potentially useful information.

The converse of mining data on the movements of large numbers of people to extract terrorist-related intelligence also deserves renewed attention—that is, the use of intelligence to restrict the movements of potential terrorists. This is already done with the use of watchlists to guide decisions by consular officers in granting visas and officers of the INS in admitting foreigners at points of entry. Although there have been well-publicized instances of the lists either not being used or being incomplete, the system generally works smoothly and has kept scores of suspected terrorists out of the United States. The best candidate for broadening the use of such procedures would be civil aviation. How was it, for example, that at least a couple of the September 11 hijackers had come to the intelligence community's attention for prior contacts with suspected terrorists and yet were able to buy tickets and board civilian airliners in the United States under their true names? Probably the only way to avoid a recurrence would be a drastic revision of aviation security that in essence would require all air passengers to undergo a background check. This strategy raises issues of privacy that also would apply to some data mining. These issues, along with the question of whether the small payoffs would be worth the high costs and the intrusion, call for public debate and extensive consideration by Congress.

Domestic Intelligence

Tradeoffs between counterterrorism and privacy abound in the collection of intelligence within the United States, which must be a major part of the overall counterterrorist intelligence function. Debates in the United States about homeland security have been slow to address the most important issues of domestic intelligence collection. Discussion of intelligence during congressional consideration of the homeland security bill of 2002 had to do with what kind of intelligence element the new Department of Homeland Security would have and how the department would relate to the FBI and the CIA. This issue need not have been controversial. The department's intelligence arm can perform the same sort of role as the State Department's Bureau of Intelligence and Research—an analytical and coordinating office that works closely with the rest of the intelligence community to meet its own department's intelligence needs.

The biggest departure the United States could take regarding counterterrorist intelligence—one that has not been a subject of congressional de-

bate—would be to create a domestic security service, separate from foreign intelligence agencies such as the CIA and NSA and law enforcement agencies such as the FBI. The United States is atypical in not having an agency comparable to MI-5 in the United Kingdom, the Federal Office for the Protection of the Constitution (BfV) in Germany, or the Public Security Investigation Agency in Japan. Collection of intelligence on foreign terrorists within their respective homelands is a major mission for these and similar agencies in other countries.

Whether to create such an agency in the United States is largely an issue of whether this mission should be left to the FBI. (The CIA would be an inappropriate place for the job, mainly because its mission of collecting foreign intelligence differs in important respects. Recruiting a foreign spy, for example, may involve persuading that person to violate the laws of his own country.) The principal argument against establishment of a new service is that the FBI, although primarily a law enforcement organization, has long had the secondary mission of collecting intelligence on persons or groups posing threats to national security. In the wake of the September 11 attacks, FBI Director Robert Mueller, through reorganization and reallocation of resources, has given increased emphasis to the collection and preemptive use of counterterrorist intelligence. Another consideration is that creation of a new service would mean one more set of organizational lines that information would have to cross—information that, given the relationship between law enforcement and the gathering of information on threats within the United States, needs to flow as freely as possible.

The main argument in favor of establishing a new service is that because the culture and expertise of the FBI center around law enforcement and the assembling of criminal cases for prosecution, the intelligence mission—no matter how much emphasis the bureau's directors place on it—will always be a secondary mission in fact if not in name. And no mission can be performed really well if it is only somebody's secondary mission. The bureau's ethos is so closely centered around law enforcement and criminal prosecutions that it remains uncertain how well-suited it is to an intelligence mission, no matter how many adjustments are made from the top. The training, skills, and promotability of FBI special agents all revolve around the criminal law function. This fact is evident in countless habits and patterns of work, such as a disinclination of FBI agents to document many substantive discussions—such documentation being second nature to an intelligence officer—out of concern about creating a written record that would be discoverable in a trial.

The traditional autonomy of FBI field offices, with the informational disconnects such autonomy can cause, also would argue for creation of a new intelligence service. Director Mueller has attempted to address this issue with

creation of a headquarters-based "supersquad" that would direct terrorist investigations that traditionally have been handled by field offices. Yet field-to-headquarters relationships may be one of the aspects of an organization's culture and operating habits that is most resistant to change. And although something like the investigation of a bank robbery usually can be handled fully within the locale of the crime, inquiries into terrorist groups—with their transnational dimensions—cannot.

Another possible reason to create a new domestic intelligence and security agency would be the symbolic value of such a major step, with all of the signals it would send regarding the nation's commitment to the agency's mission and the resources and legal powers necessary for it to do its job properly. It would represent a break with past shortcomings and a sea change in national priorities. A new organization would be unencumbered by the baggage of the CIA and the FBI, including past controversies involving alleged abuses or overstepping of bounds and popular perceptions of past failures.

Regardless of whether the domestic counterterrorist mission is performed by a new service or by a reoriented FBI, many other questions about the mission will be unavoidable topics of controversy and appropriate topics of debate. Besides the ubiquitous matter of resources, there are issues involving legal authorities to monitor activity and conduct searches and seizures. Skepticism that met Attorney General John Ashcroft's widening of the FBI's monitoring powers in May 2002 reflected deep and longstanding American reservations about such authorities.[26] Another question is whether U.S. citizens and noncitizens should be targeted in the same way. The American public might be willing to support more intrusive investigative powers aimed at noncitizens (who probably include most of the terrorist threats). Yet even foreign terrorist groups can enlist—and, to a limited degree, already have used—U.S. citizens.

There also is the problem of where investigative leads come from. It may be somewhat easier to search a haystack in one's own yard than a haystack elsewhere, but it is still a haystack. The criticism of the Terrorism Information and Prevention System (TIPS)—an effort to encourage reporting by individual citizens of suspicious circumstances or behavior that could have terrorist implications—highlighted the biggest barrier to more extensive domestic intelligence collection: Americans don't like to be spied on, by either their government or their fellow citizens. For many Americans, TIPS carried the odor of an East German-style system of friends and family members "ratting" on each other.

Another subject that already has an odor in the United States but cannot be avoided in considering how to focus the search of the haystack is profiling on the basis of religion, race, or ethnicity. The best profiling systems use other indicators that are less controversial and more closely correlated

with the behavior one is trying to detect. In trying to narrow the gargantuan task of finding as-yet-unfound threats in a nation of nearly 300 million people, however, an uncomfortable fact is that religion and ethnicity would have some search-narrowing value. Somehow that fact will have to be dealt with in any enhanced domestic intelligence effort.

Above All, Do No Harm

The intensity of pressure on the intelligence community to be seen doing things in new and different ways, coupled with the meager prospects that such change actually will reduce the chance of more major terrorist attacks, means that the challenge for U.S. intelligence will be not only to do the best possible job of collecting and analyzing information about terrorism but to respond to the demand for change in ways that avoid doing more harm than good. One of the most important "risks" for the CIA and the rest of the intelligence community is the political risk of standing up to these short-term pressures to avoid undermining long-term effectiveness.

Since September 11, U.S. intelligence agencies have devoted an even larger proportion of their resources than before to counterterrorism. This reallocation has been the kind of nimble shift that the CIA in particular often—and mistakenly—has been criticized for not being able to do. The shift means pulling analysts and collectors off other important subjects, however. The House Intelligence Committee expressed concern about this shift in its report accompanying the intelligence authorization bill for fiscal year 2003, noting that the "significant and inventive" counterterrorist efforts that the intelligence community had under way were being achieved by shifts of personnel "that create gaps in coverage and understanding in other areas of national security interest."[27] In responding to the inevitable pressures to move more resources to counterterrorism, the intelligence community must be careful not to denude itself in these other areas. The costs of doing so would be felt not only with other U.S. foreign policy interests but, over the long term, with counterterrorism itself. Although understanding political stresses and socioeconomic patterns in foreign lands does not bear the "counterterrorist" label, this work often addresses the conditions that tend to breed terrorists and therefore is important in anticipating future terrorism and supporting U.S. policy efforts to do something about it.

Another hazard involves the rules and restrictions under which the intelligence community operates and how the mood of the moment, in which counterterrorism has become an overriding public priority, has changed those rules. The September 11 attacks appear to have swept aside many old suspicions and concerns about the country's national security agencies. The

changes are reflected in such things as the congressional directive regarding recruitment guidelines and the omnibus counterterrorist legislation enacted in October 2001 that, among other things, gives the CIA access to grand jury testimony.[28] The public mood will change again, however. If a couple of years go by with the United States successful enough and fortunate enough to avoid another major terrorist attack, counterterrorism will no longer be an overriding priority. Human rights, privacy, and similar issues will get renewed attention. Then what? What happens to the "incentivized" intelligence officer who takes the risk of making a recruitment that becomes controversial, and how will his agency be viewed after the members of Congress who changed the rules have moved on to other committee assignments? And does a step such as giving intelligence agencies access to grand jury records contain the seeds of future congressional inquiries reminiscent of the Church and Pike committees of the 1970s?[29] The changes may be warranted, and there is no reason to anticipate abuses. Those making the changes should remember, however, that among the most effective weapons the United States has in fighting terrorism is the long-term strength of its intelligence agencies, based in part on their integrity and the trust they have with the American people.

Public confidence in the counterterrorist role of intelligence agencies also is put at risk when that role is misappropriated to serve purposes other than saving lives from terrorism. The very prominence of counterterrorism in the wake of September 11 has increased the temptation to misuse the counterterrorist issue in this way. Supporters of the war against Iraq did so when they exploited the militant post–September 11 mood of the American public to muster support for the war, which they had long favored chiefly for reasons other than counterterrorism.[30] Selling the war involved playing up any link that could be found between Saddam Hussein's regime and terrorism—especially between the regime and al-Qaeda. Proponents of the war used intelligence not to identify threats and inform policymaking but to justify a policy decision that already had been made.

The intelligence community withstood the policy pressures fairly well. Its treatment of Iraq and al-Qaeda did not go beyond detailed description of the minimal and inconclusive "links" between the two—as was evident on a careful reading of the administration's only public statement on Iraq that had a direct intelligence community input: Secretary of State Powell's presentation to the United Nations Security Council in February 2003.[31] Nonetheless, the Iraq episode damaged the intelligence community's ability to play its part in counterterrorism. Servicing the administration's public relations requirements on this issue consumed vast amounts of time and attention on the part of counterterrorist specialists, who thereby were diverted from their main mission of locating and countering actual and impending terrorist threats.

The American public's understanding of the role of state sponsors in international terrorism was badly distorted, in a way it would not have been if intelligence had been used publicly in a more straightforward manner. Most important, as postwar difficulties in Iraq became increasingly apparent and the failure to find weapons of mass destruction caused alleged misuse of intelligence to become a major issue, the integrity of the intelligence community was called into question. This outcome will make public trust harder to win the next time intelligence identifies a major terrorist threat, even if the threat is real and the assessment of it unpoliticized.

Conclusion

The most useful thing that Americans can do about U.S. intelligence assets in the campaign against international terrorism may be to acquire a realistic appreciation for what those assets can and cannot accomplish. It is important to understand the small chance of obtaining critical inside information on the next terrorist plot and the multitude of other ways intelligence contributes to counterterrorism. Such understanding would guide strategy on how much reliance to place on the intelligence community's "first line of defense" against terrorism and how much needs to be done by the other lines. It would help to avoid reinventing wheels that the intelligence community invented some time ago and focus attention on areas—particularly a more comprehensive integration of intelligence with nonintelligence data—where there is at least a modest chance of major new initiatives yielding results. Moreover, clearing away misconceptions would sharpen the focus on important issues—particularly what compromises Americans are willing to make to their privacy and liberties to facilitate the collection of information about possible threats in their own homeland—that still need debate.

Almost all of the functions of, and possible new initiatives in, counterterrorist intelligence discussed in this chapter rest on strong and knowledgeable public support. Such support is critical for resources, of course, in the form of appropriations by Congress. Public acceptance also would be vital to implement the kinds of procedures necessary for an expanded domestic intelligence collection effort to be effective. Although less immediately apparent, the amount of public backing that U.S. officials have when they solicit cooperation from foreign governments also helps to determine how successful such solicitations are.

The upsurge in Americans' support for counterterrorism in the wake of the September 11 attacks provides the principal grounds for optimism about realizing the full potential of what intelligence—despite all of its continuing limitations—can contribute to the larger counterterrorist effort. The

markedly increased success since the attacks in freezing of terrorist financial assets, for example, is due not to the intelligence suddenly getting better but to the national strength of commitment that has enabled U.S. officials to pound on the desks of foreign officials and insist that they act on the intelligence that was already available. And Operation Enduring Freedom in Afghanistan was the most forceful possible example of acting on intelligence about the principal source of the principal terrorist threat of the day. To the extent that American interest in counterterrorism can be sustained longer than after previous spikes in such interest, there will be more successful applications of intelligence to the problem of international terrorism, beyond the eternally hoped-for uncovering of details of the next plot.

Notes

The views in this article are the author's and not those of any government agency.

1. *Report of the Accountability Review Boards on the Bombings of the U.S. Embassies in Nairobi, Kenya and Dar es Salaam, Tanzania on August 7, 1998.*

2. Most speculation was exactly that, rather than rigorous analysis. The best analysis of the subject is Richard A. Falkenrath, Robert D. Newman, and Bradley Thayer, *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack* (Cambridge, Mass.: MIT Press, 1998). Related scholarly treatments include Jessica Stern, *The Ultimate Terrorists* (Cambridge, Mass.: Harvard University Press, 1999); Jonathan B. Tucker (ed.), *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons* (Cambridge, Mass.: MIT Press, 2000); and Gavin Cameron, *Nuclear Terrorism: A Threat Assessment for the 21st Century* (London: Macmillan, 1999).

3. Cf. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, N.J.: Princeton University Press, 1949), especially chap. 4, and Richard K. Betts, "Warning Dilemmas: Normal Theory vs. Exceptional Theory," *Orbis* 26 (winter 1983): 828–33.

4. Dan Balz and Bob Woodward, "America's Chaotic Road to War," *Washington Post*, 27 January 2002, A11.

5. See testimony by George Tenet, U.S. Senate Select Committee on Intelligence, *Worldwide Threat 2002: Current and Projected National Security Threats to the United States*, 107th Congress, 2d session, 6 February 2002.

6. House Report 107–219, on HR 2883.

7. Karen DeYoung and Walter Pincus, "In Bin Laden's Own Words," *Washington Post*, 14 December 2001, A1.

8. For the president's statement, see his speech on 6 June 2002 proposing creation of a Department of Homeland Security, available at www.whitehouse.gov/news/releases/2002/06/20020606–8.html. On the congressional investigation, see Dana Priest and Juliet Eilperin, "Panel Finds No 'Smoking Gun' in Probe of 9/11 Intelligence Failures," *Washington Post*, 11 July 2002, A1.

9. Statement by DCI George Tenet, U.S. Senate Select Committee on Intelligence, *Worldwide Threat 2001: National Security in a Changing World*, 107th Congress, 1st session, 7 February 2001.

10. Barton Gellman, "A Strategy's Cautious Evolution," *Washington Post*, 20 January 2002, A17.

11. Department of Defense, *Report to the President and Congress on the Protection of U.S. Forces Deployed Abroad* (August 1996), Annex A.

12. *Report of the Accountability Review Boards.*

13. The Bush administration subsequently was reported to have moved to a more general policy of military preemption against possible terrorist threats. Thomas E. Ricks and Vernon Loeb, "Bush Developing Military Policy of Striking First," *Washington Post*, 10 June 2002, A1.

14. See, e.g., *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, report of the Commission on the Roles and Capabilities of the United States Intelligence Community (Washington, D.C.: U.S. Government Printing Office, 1996), 47–59; and Mark W. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2000), 24–32, 130–31.

15. Ashton B. Carter, "The Architecture of Government in the Face of Terrorism," *International Security* 26 (winter 2001/02): 18–19; and Ashton B. Carter, John Deutch, and Philip Zelikow, "Catastrophic Terrorism: Tackling the New Danger," *Foreign Affairs* 77 (November–December 1998): 80–94.

16. Quoted in Chuck McCutcheon, "Fixing U.S. Intelligence: A Cultural Revolution," *Congressional Quarterly Weekly*, 6 October 2001, 2307.

17. Eric Schmitt, "Job Seekers Flood Spy Agencies," *New York Times*, 22 October 2001, B7.

18. Thomas Powers, "The Trouble with the CIA," *New York Review of Books*, 17 January 2002, 31.

19. The most formal expression of this view is in *Countering the Changing Threat of International Terrorism*, report of the National Commission on Terrorism (June 2000), 8.

20. Ibid.

21. Frank J. Ciluffo, Ronald A. Marks, and George C. Salmoiraghi, "The Use and Limits of U.S. Intelligence," *Washington Quarterly* 25 (winter 2002): 69.

22. Section 403, Intelligence Authorization Act for fiscal year 2002.

23. On the theme that further changes to the intelligence community are likely to yield only small payoffs, see Richard Betts, "Fixing Intelligence," *Foreign Affairs* 81 (January–February 2002): 43–59.

24. Ronald Kessler, "Double the Size of the FBI," *Washington Post*, 15 June 2002, A23.

25. See the comments of former INS Commissioner Doris Meissner in "On the Fence" (interview), *Foreign Policy* 129 (March–April 2002): 24.

26. Neil A. Lewis, "Ashcroft Permits F.B.I. to Monitor Internet and Public Activities," *New York Times*, 31 May 2002, A18.

27. Quoted in Walter Pincus, "House Votes Billions for Intelligence: Panel Says Anti-Terror Fight Creates 'Gaps' in U.S. Coverage," *Washington Post*, 26 July 2002, A11.

28. USA Patriot Act, P.L. 107–56, Section 203.

29. Cf. Tim Weiner, "The C.I.A. Widens Its Domestic Reach," *New York Times*, 20 January 2002, 4.1.

30. Joseph Cirincione, "Origins of Regime Change in Iraq," *Carnegie Endowment Proliferation Brief* 6, no. 5 (March 19, 2003).

31. The text of Secretary Powell's statement is at www.state.gov/secretary/rm/2003/17300.htm.