

**Statement of  
Paul R. Pillar  
to the Joint Inquiry of the  
Senate Select Committee on Intelligence and  
House Permanent Select Committee on Intelligence  
8 October 2002**

Mr. Chairman, I thank the committees for their invitation to contribute to this hearing on lessons from past US experiences in countering international terrorism. My perspectives are those of an intelligence officer who worked on counterterrorism for much of the 1990s, as chief of assessments in the DCI Counterterrorist Center and then as deputy chief of the center, and also as someone who has looked at counterterrorism more broadly from the perspective of a policy analyst. I commend the committees for holding a hearing with the purpose this one has. The public discussion of counterterrorism over the last year naturally has focused on the events of last September, on how the threat that led to it was handled, and in particular on any errors in the handling of that threat. While that kind of examination is of course necessary, the question of what might be done better in the future to reduce the chances of terrorist strikes against our nation's interests cannot be answered solely through examination of a single incident, however tragic and traumatic. We can begin to answer it only by understanding what has been tried in the past, what changes in our approach have already taken place, and what possibilities and limits have already been demonstrated.

**Persistent Challenges to Intelligence**

The first lesson is that the principal characteristics of the terrorist threat we face today, and the challenges for intelligence that those characteristics pose, have been with us for quite some time. September 11<sup>th</sup> obviously was an extraordinary event in terms of the death toll and the resulting deep impact it had on our nation, but the difficulties that operation presented to intelligence, and to law enforcement, were all too typical of what we have repeatedly faced in the past. Terrorist groups—or more specifically the parts of them that do the planning and preparations for terrorist attacks—are small, highly secretive, suspicious of outsiders, highly conscious of operational security, and for these reasons extremely difficult to penetrate. Terrorist plots can be, and generally are, kept under wraps through fairly simple precautions on the part of the terrorists, such as doing their planning behind closed doors, not communicating through means that can be intercepted, and living lives that do not draw attention to themselves.

The collection challenges go even farther. The intelligence target is not just a fixed set of known terrorists whose secrets we have had to try to uncover. It is anyone—even if not a card-carrying member of a known terrorist group and even if not having been involved in previous terrorist activity—who may use terrorist techniques to inflict harm on US interests.

Along with the collection challenges are the analytical ones. The material that counterterrorist analysts have had to work with has always consisted of voluminous but fragmentary and ambiguous reporting, much of it of doubtful credibility, that provides only the barest and blurriest glimpses of possible terrorist activity. The analysts have

long been faced with blizzards of flags or dots—whatever one may choose to call them—that could be pieced together in countless ways. If pieced together in the most alarming ways, the alarm bell would never stop ringing.

### **Tactical and Strategic Intelligence**

Although the task of tactical warning has always run up against these formidable challenges, the scraps and fragments that intelligence collects often have enabled analysts to offer warning of a more strategic nature—that the terrorist threat from certain kinds of groups, or in certain countries or regions, or against certain categories of targets, or in response to certain kinds of events is higher than it is elsewhere. The result has been a pattern in the intelligence community's performance that has been noted, for example, in the inquiry led by General Wayne Downing into the bombing of Khobar Towers. That pattern—a lack of tactical warning of the attacks, but good strategic intelligence about the underlying terrorist threats—does not result from different cohorts of intelligence officers making the same mistake, or the intelligence community stubbornly refusing to correct some systemic flaw that these past attacks have revealed. It is what you get when earnest efforts are made to extract what can be extracted from this extremely hard intelligence target.

Certainly the intelligence community must spare no effort to obtain tactical intelligence on future terrorist attacks against US interests. Even a small chance of obtaining the rare tactical nugget that might enable a future plot to be foiled is worth major effort. But years of experience teach us that even if high priority is given, as it has been, to the development of sources for that kind of specific information, and even if considerable imagination and resources are applied, as they have been, to that task, truly well-placed sources in terrorist groups—the kind that can yield plot-specific information—will always be rare. And partly because of that, we can expect to obtain specific information on some, not all, of the terrorist plots against our nation's interests. If the US intelligence community never failed to obtain specific warning of such plots, then there would never again be any anti-US terrorism. That is a goal for which we must strive, but it is not a goal we can realistically expect to attain.

A corollary lesson is that the United States should avoid overly heavy reliance on intelligence to provide tactical warning. The panel led by Admiral William Crowe that studied the attacks on the embassies in 1998 noted an unfortunate tendency among security managers toward such excessive reliance on tactical intelligence. It is an understandable tendency, since ramping up security measures only when a threat is present is more affordable and less disruptive than keeping them in effect continuously. Intelligence officers share a responsibility for countering that tendency, by reminding consumers what we don't know as well as what we do.

As important as tactical warning is, and even though it gets disproportionate attention in most discussions of the role of intelligence in counterterrorism, it represents only a fraction of what intelligence has contributed through the years to counterterrorism, including contributions that have saved lives. Strategic intelligence can be even more useful than the tactical as an input to decisions on security countermeasures, many of which involve costly long-term efforts to respond to continuing threats rather than to a single plot.

One subject that received strategic attention from the intelligence community in the 1990s was threats to the US homeland. The 1993 attack against the World Trade Center was a key event. It did not generate anything close to the level of public attention and concern that would be seen eight years later—that's the difference between an attack that kills six people and one that kills 3,000. But to intelligence community analysts the larger threat to the homeland was apparent. The goal of the World Trade Center truck bombers had been to topple the twin towers and kill thousands.

The community's work on this subject culminated in 1995 in a National Intelligence Estimate—the most formal and fully coordinated form of intelligence assessment, one that is personally approved by the DCI and heads of community components. This Estimate was probably the single most conspicuous piece of intelligence analysis that the community produced on terrorism during the mid-1990s. The sole subject of the Estimate was foreign terrorist threats to the US homeland. The FBI, along with CIA and other intelligence community agencies, participated fully in preparation of the Estimate, so that it would reflect the Bureau's information on the foreign terrorist presence in the U.S. as well as the intelligence available to CIA and others.

As was noted in one of the committees' staff reports, this Estimate addressed civil aviation as an attractive target that foreign terrorists might strike in the United States. This particular aspect of the Estimate was the subject of subsequent efforts, involving the DCI Counterterrorist Center, the FBI, the National Intelligence Council, and the FAA, to sensitize relevant consumers to the threat. The FAA arranged a set of special briefings for representatives of the aviation industry, at which senior CIA and FBI counterterrorist specialists presented much of the material in the Estimate, as part of an effort to persuade the industry of the need for additional counterterrorist security measures for domestic civil aviation.

What is the lesson to be drawn from this episode, apart from the direct one that the intelligence community and the FBI were working closely with the relevant regulatory agency as early as the mid-1990s to call attention to the foreign terrorist threat to domestic civil aviation? I think it has to do with how much our national willingness to respond with things like expensive new security measures depends on the reality of past tragedies more than projections of threats that have not yet materialized. The intelligence community has a duty here. As any new intelligence analyst is taught, what matters is not just to make correct predictions and hit the right notes—which may look good in post-mortems—but to beat the drum loudly enough about impending threats to have some chance of making an impact on policy. Maybe the intelligence community could have beaten the drum even harder in this instance, but it is tough to compete with what had been, before September 11<sup>th</sup>, many years of civil aviation operations in this country that had been virtually untouched by terrorism.

### **Terrorist Tactics**

Threats to aviation involve a particular terrorist tactic, and prognostication of tactics, like plot-specific tactical warning, gets a great deal of attention in discussions of counterterrorist intelligence. But divining the tactic that terrorists will use in the next major attack is not the biggest contribution that US intelligence has made in past years, and I do not expect it to be in the future. Terrorists vary their tactics, as they look at

security measures and go to where the vulnerabilities are, and as they try to keep the good guys off balance and guessing. Al-Qa'ida alone has used truck bombings, a waterborne attack, and hijacking. Intelligence has a role in pointing out any emerging patterns in what terrorists seems to be considering in the way of tactics and targets. But over the long term the biggest counterterrorist payoffs probably will come less from foiling tactics than from foiling terrorists. Counter one technique and you make it more difficult for terrorists to use that tactic, perhaps inducing them to look to other methods. Disrupt a terrorist cell and you prevent that cell from attacking any target with any tactic.

Over the last several years there has been particular attention given to possible terrorism using chemical, biological, radiological, or nuclear means—CBRN terrorism, to use the common abbreviation. In public discussion, there developed a widespread tendency to equate the danger of terrorism against US interests, and particularly against the US homeland, with mass casualty CBRN attacks. Almost every response exercise, for example, involved a chemical or biological scenario. I do not belittle the CBRN threat, which may be increasing—and not just with al-Qa'ida, whose ambitions in the CBRN area have been well established. But the attention given to this one particular set of possible terrorist tactics since the mid-1990s outstripped, as I wrote prior to 9/11, what terrorists were actually doing operationally. The U.S. intelligence community was probably no more guilty, and perhaps less guilty, than outside commentators of giving disproportionate attention to this one possible terrorist technique, and in any case the community needs for other reasons to monitor closely CBRN developments worldwide. What captures the attention of those outside the community affects the use of resources inside it, however, if only in the form of time taken to answer questions. The broader preoccupation with possible CBRN terrorism continued through the series of conventional terrorist attacks against US targets: New York, Riyadh, Khobar, Nairobi, Dar es Salaam, Aden, and finally September 11<sup>th</sup>, which was the most dramatic possible demonstration that one could achieve mass casualties, including in the US homeland, without using CBRN. I might add that the other terrorist attack in the United States last fall—the anthrax letters—demonstrated that one can use CBRN without inflicting mass casualties.

### **Evolution of the Intelligence Community's Response**

The record of the US intelligence community changing in response to the threat from international terrorism goes back farther than the end of the Cold War—back to the 1980s, when the main US concern was with Hizballah's activities in Lebanon, including the bombing of our embassy and the Marine barracks and years of hostage-taking, as well as the terrorist activities of certain states. The community's principal response at that time, and in many ways still its most important response, was the creation of the DCI Counterterrorist Center, or CTC, in 1986. This step was a bureaucratic revolution. It involved slicing across longstanding lines on the organization chart, bringing analysts and operators to work more closely together than they ever had before, and benefiting from the synergy that comes from having people with different skills and specialties attacking the same high priority problem together. The success of the concept is reflected in the fact that CTC became a model for other centers that subsequently were established to address such issues as proliferation and narcotics.

Further refinements were made in CTC in subsequent years. One for which I am proud to claim personal credit was the creation of a permanent cadre of counterterrorist analysts, replacing an earlier system in which the analysts working on counterterrorism were on loan from other offices, which continued to control their careers. There now are analysts moving into CIA's Senior Analytical Service as counterterrorist experts. There were also reconfigurations within the Center to increase the synergy further. This particularly included the creation of a multidisciplinary unit, a sort of center within a center, focused exclusively on Usama Bin Ladin. This step was taken well before Bin Ladin became a household word.

Another refinement in CTC was the increased representation of agencies other than CIA, particularly but not exclusively law enforcement agencies such as the FBI. This was a recognition of how important the intelligence-law enforcement nexus is to counterterrorism. A lot has been written and said over the past year about this relationship. I find elements of truth in much of it, having to do with cultural distinctions and the like, but I also find much of it dated. The relationship, specifically the FBI-CIA relationship, improved greatly during the 1990s. This was partly due to a commitment at the top of each agency to make it work. It was also due to the cross-assignments of personnel about which you have heard from other witnesses, some of whom were in those assignments. There were also more informal methods used to learn about each other's business. Along with improved cooperation in Washington, there was an expansion of collaboration in the field. The increase in the number of FBI overseas representatives, or legatts, was welcomed by CIA because it made that collaboration easier. And there was increased communication between CTC and Justice Department prosecutors working on key terrorist cases, and particularly with the Southern District of New York, where so many of those cases were.

Along with these changes involving personnel and organization, CTC's methods and operational strategy also evolved. An increasing amount of work was devoted to supporting the law enforcement missions of determining responsibility for terrorist attacks and tracking down fugitive perpetrators. A long-running task force established after the 1993 World Trade Center bombing to support the FBI's work on that case became a sort of model for support work on other cases. Efforts to recruit well-placed unilateral sources continued to have high priority, but CTC developed during the 1990s a strategy that recognized that although information about specific terrorist plots was rare, other information about suspected terrorists and their activities was more feasible to acquire. The strategy was to work with many foreign government partners to disrupt terrorist cells using whatever information we could collect about them. Most terrorists commit other illegal activity besides terrorism, and this became the basis for many arrests, interrogations, and other disruption initiatives—akin to nailing Al Capone for tax evasion. This type of disruption work must continue to be a major part of US counterterrorist efforts. It is slow, it is incremental, and it does not yield many spectacular, highly visible successes. But I am convinced that by impeding the operations of terrorists it has prevented some terrorist attacks and has saved innocent lives.

The main lesson I hope the committees draw from this capsule history is that there already has been a long and substantial evolution of the intelligence community's approach to tacking international terrorism. Most of the innovations worth trying have

already been tried. Most of the major organizational changes that needed to be made have been made. I'm sure all of us in this room wish there were some additional change or set of changes that would give us assurance that something like September 11<sup>th</sup> would not happen again. But I am not aware of a step that would provide that kind of assurance, and I don't believe there is one, even though there clearly is room for additional improvement as long as our counterterrorist batting average is not 1.000, which means indefinitely. In searching for ways to avoid recurrence of the sorts of errors and omissions that have received so much attention in the September 11<sup>th</sup> case, we should try not to reinvent wheels already invented or, even worse, to undo beneficial adjustments made in the past. We should also be careful not to give the American people any unjustified sense that with new changes the problem of international terrorism has been solved.

### **Counterterrorist Instruments**

I was asked to comment on general US strategies for countering terrorism in the past, and the benefits and drawbacks of counterterrorist instruments.

The main lines of US counterterrorist policy remained fairly constant for most of the decade prior to September 11<sup>th</sup>, including the longstanding declared principles of making no concessions to terrorists, bringing terrorists to justice, isolating and pressuring state sponsors of terrorism, and bolstering the counterterrorist capabilities of countries that work with the United States. Beyond those principles, the strategy could be described as one of making use of all of the instruments available, in recognition that each instrument has something to offer but also limitations. It was mostly a pragmatic effort to use tools whenever they offered a reasonable chance of being effective and the risk of using them was low.

I have already commented on the contributions and limitations of intelligence. Another major instrument, prosecuting terrorists through the US criminal justice system, has both its advantages and its limitations as applied to counterterrorism. The advantages include the direct one of taking individual terrorists out of circulation in a manner consistent with the laws we apply to our own citizens and the indirect ones of a possible deterrent effect on other terrorists and the demonstration of US resolve afforded by a public trial. The limitations include the uncertainty of the deterrent effect, the higher standards involved in building a legal case rather than an intelligence case to prove someone is a terrorist, and the fact that terrorist leaders are less likely to be caught than the low-level people who carry out their plans. The criminal justice system must continue to be a major instrument of counterterrorism, although probably not enshrined at a higher level of importance than the other instruments, as it seems to have been in the past. We also need to give greater consideration to what the courts of other nations can do, even with terrorists indictable in the United States. Taking terrorists out of circulation and making them pay for their crimes is more important than who accomplishes those tasks.

The use of military force offers the advantage of being the most dramatic possible demonstration of US resolve to fight terrorism, as well as offering some deterrent value and possibly some physical destruction of terrorist infrastructure. The limitations are also readily apparent. Armed force may provoke rather than deter some terrorists, who may welcome the use of force for reasons of propaganda, recruitment, and keeping their own

rank-and-file motivated. There are always the risks of broader diplomatic and political repercussions from the use of military force for any purpose. And perhaps most significantly, the terrorists most threatening to the United States provide few good military targets. The terrorist preparations that matter most tend to take place not in camps that can be bombed but in apartments in places like Hamburg or Beirut or Kuala Lumpur. The significant success of Operation Enduring Freedom in Afghanistan provides occasion for renewed consideration of the military instrument in counterterrorism. We should remember, however, that there has never been another place comparable to Afghanistan as a training ground for tens of thousands of extremists over two decades, as the headquarters of a deadly group like al-Qa'ida, and as the seat of a regime—the Taliban—that was more closely in partnership with terrorists than any other in the world.

Other instruments—offensive, counterterrorist instruments, not just security countermeasures—also are important and must continue to be used to the fullest. Diplomacy is important in many ways, ranging from maintaining international pressure against state sponsorship of terrorism to getting help in acting against individual terrorists. The interdiction of terrorist money produced only meager results for most of the past decade, but the great increase in freezing of terrorist assets since September 11<sup>th</sup> has shown what can be accomplished when such efforts are backed up by a determined nation. Our basic approach to the use of the various counterterrorist instruments must be: use them all, and use them together.

### **Recommendations**

I was asked for recommendations for improving the US Government's performance in fighting terrorism. I have made some suggestions in my other writings, but let me focus on a few matters of most direct concern to these committees. In doing so I want to underscore that, for the reasons I mentioned earlier, even major new efforts or initiatives are apt to yield only modest results.

First, it is vital to have sustained, long-term public support for what the intelligence community needs to do in counterterrorism—with everything that implies regarding resources. The main impact that the various attacks on US targets had on the work of the Counterterrorist Center over the past decade and a half was that those were the times when public interest in the subject spiked and resources went up. When public interest waned, as time passed without a major attack, resources were tighter. That was certainly the case after the terrorist concerns of the 1980s faded in the public consciousness and remained the case for most of the first half of the 1990s. The vital, painstaking work of taking apart terrorist groups and terrorist infrastructures is long-term work, and it cannot be done with the kind of ups and downs in support that have occurred in the past.

Second, we probably should try to make more extensive use of multiple sources of data, including nontraditional sources, to detect possible terrorist activity. By this I mean not just using watch lists and checking names while working on individual cases, but rather a broader exploitation for intelligence purposes of such things as travel and immigration data. I have always thought that trying to do this involved immense practical difficulties, ranging from the use of multiple names to problems in getting the information from the private and public sources that own it. I still think so. It would

involve looking through huge haystacks with only a chance of finding a few needles. But the standards for return on investment in counterterrorism changed on 9/11, and perhaps this is an avenue we need to explore further.

Third—and this goes far beyond what the intelligence community itself can accomplish—we must nurture foreign relationships to get the cooperation of foreign governments that is so vital to a host of counterterrorist matters, especially including intelligence matters. Of course we need to continue to make every effort to develop unilateral intelligence sources. But in counterterrorism, we will always be—for several geographic, cultural, and jurisdictional reasons—more dependent on foreign partners than with almost any other intelligence topic. That is not a weakness; it is something to cultivate and exploit. We need our partners for information, and we need them to carry out most of the arrests, the raids, the confiscations, the interrogations, and the renditions that are involved in dismantling terrorist groups. This means we need to give them the incentives to cooperate, and if necessary the assistance in developing the capabilities to do so.

Finally, we should take a broad view of counterterrorism and recognize how much future terrorism against US interests will depend not just on what is done by people at the CIA or FBI who have counterterrorism as part of their titles. Counterterrorism involves far more than learning the secrets of the next terrorist plot or erecting security measures around what we think is the next terrorist target. It also involves the motivations for groups to use terrorism, and the conflicts and conditions that lead some people to join terrorist groups—even though there always will be some, like Bin Ladin, who seem determined to do us harm regardless of motives or conditions. This broad view obviously gets into many foreign policy issues. But the lesson for intelligence is that as more priority is given to particular counterterrorist accounts, we should not denude ourselves of coverage in other areas that bear on possible future terrorism. The intelligence community has a responsibility not only to go after the current al-Qa'ida but to be aware, early on, of the next one—whatever form such a future terrorist threat might take—and of the conditions that might lead such a threat to emerge.