

# Assessing U.S. Counterterrorism Efforts

By L. Paul Bremer III

---

**This article examines the latest commission report recommendations, along with subsequent developments.**

---

International terrorists' attacks against the United States have changed dramatically in recent years, becoming more deadly and, of particular concern, striking within the country's borders. Examples include the 1993 bombing of the World Trade Center, the thwarted attacks on New York City's Lincoln and Holland tunnels in 1993, and the 1995 plot to blow up 11 American airliners. Crowds gathering to celebrate the millennium were almost certainly the target for the explosives found in a car at the U.S.-Canada border in December 1999. In fact, the 1999 annual report of the Canadian Security Intelligence Service cites the border arrests as an example of today's threat: that of "an international ad hoc coalition of terrorists" who "have expressed the intention of causing harm to Americans and their allies."

Overseas, meanwhile, more than 6,000 casualties were caused by just three attacks: the bombings of military barracks in Saudi Arabia in 1996 and of U.S. embassies in Kenya and Tanzania in 1998. If three attacks with conventional explosives could injure or kill so many, imagine the consequences of an attack using a nuclear, biological, or chemical weapon. What would happen if a release of radioactive material made Chicago's waterfront uninhabitable for 50 years, or if a biological attack infected passengers at Dallas/Fort Worth International Airport with a contagious disease?

These scenarios are entirely possible: Five of the seven countries the U.S. government considers to be terror-supporting states are working on such weapons, and individual terrorist groups are also seeking weapons of mass destruction.

Congress established the National Commission on Terrorism in 1999 to assess U.S. efforts to combat international terrorism and to make recommendations for change. In a report issued last year, the commission notes that, although many important efforts are underway, additional steps are necessary for the United States to protect its citizens. The following overview highlights the commission's recommendations as well as new developments since the commission issued its report.

## **Intelligence.**

One of the commission's central recommendations is that the United States improve its intelligence efforts in determining who the terrorists are and what they are planning. Top-flight intelligence on terrorists can be a life-and-death matter. For instance, intelligence work that included excellent cooperation with Jordan thwarted large-scale overseas attacks on Americans at the end of 1999. But such successes should not obscure the need for doing more.

*The CIA.* The commission found that efforts to gather information about terrorist plans and disseminate it to analysts and decision-makers in the federal government are often stymied by bureaucratic and cultural obstacles. For example, to recruit a member of a terrorist organization as a source, a CIA field officer faces a daunting series of reviews by committees at the agency's headquarters. This extensive process is designed to reduce the risk from such a recruitment to as near zero as possible. Because this process is so time-consuming and effort-intensive, however, the potential source may not still be willing to provide information by the time he or she is approved, or an attack may have already occurred.

The commission recommends that these rules regarding the recruitment of terrorist spies be rescinded because the testimony it heard was unanimous, unambiguous, and conclusive: The guidelines constitute an impediment to effective intelligence collection. Case officers in the field told the

commission that they do not attempt to recruit such informants because of the elaborate approval system they must follow. Instead, they seek easier recruitment targets. The commission concluded that CIA field officers should be as free to use terrorist informants as prosecutors in America are to use criminal informants.

*The FBI.* Also needed are more vigorous intelligence collection efforts by the FBI against foreign terrorists working in America and better dissemination of that information. The FBI's role in terrorism intelligence is increasingly significant, and it is essential that the Bureau employ the full scope of its authority in collecting that information.

The commission found that the guidelines from the Attorney General that govern when the FBI can open a preliminary inquiry or a full investigation are unclear (they are more than 40 pages long). Agents testifying before the commission said that they were often uncertain as to whether the circumstances of a particular case met these criteria.

This lack of clear direction has contributed to a risk-averse culture in the FBI. Thus, the commission recommends that the Attorney General and the FBI director clarify the application of the guidelines, specifically with regard to the facts and circumstances that merit the opening of a preliminary inquiry or a full investigation.

Another problem affecting the FBI's terrorism investigations is the cautious approach generally taken by the Department of Justice's Office of Intelligence Policy and Review (OIPR) in reviewing FBI applications for electronic surveillance of international terrorism targets. The commission concluded that, when the OIPR reviews these applications (before they are submitted to a court), it is mandating a higher standard than that required by the Foreign Intelligence Surveillance Act (FISA).

The FISA establishes that the court may order a wiretap if there is probable cause to expect that the target may be involved in terrorism. The OIPR has repeatedly gone beyond the probable cause standard, requiring the FBI to provide additional information before forwarding the Bureau's request to the FISA court. For instance, the Justice Department itself found that the OIPR was needlessly restrictive in its interpretation of the statute in its report on the Wen Ho Lee case.

In effect, the OIPR has been short-stopping FBI applications and usurping authority that belongs with the courts. Therefore, the commission recommends that the Attorney General direct that the OIPR not require information in excess of what is mandated by FISA's probable cause standard as a prerequisite to the application being forwarded to a court for consideration.

Problems continue past the information-collection phase. After the FBI collects intelligence information, technology shortfalls and institutional practices limit efforts to use it effectively and disseminate it to those who need it, such as intelligence analysts and policy makers.

To remedy part of this situation, the commission recommends that increased resources be given to the FBI for its technology needs, particularly in the area of encryption. More than 50 percent of the FBI's field offices report that they have encountered encrypted information related to criminal, counterintelligence, or terrorist activity. Many times, the FBI cannot gain timely access to the text of lawfully seized evidence because of decryption difficulties. Other FBI technology needs include information-processing equipment and communication systems able to move information around the Bureau rapidly and securely.

Decrypted information is only valuable, however, if it reaches the people who need it. Dissemination of general intelligence information traditionally has not been an important part of the FBI's mission. Though the Bureau is good at disseminating specific threat information, general knowledge sharing is not a high priority.

In fact, if the information is not specific enough to require issuing a warning or is not relevant to an investigation or prosecution, it may not even be reviewed. Information collected in field offices often is not sent to FBI headquarters, let alone to the broader community of intelligence analysts. That practice

is unwise, as the uncirculated information could prove key in preventing a future attack if it were properly reviewed.

The World Trade Center (WTC) case is an example of this problem. In 1992, Ahmed Mohamed Ajaj entered the United States with Ramzi Yousef. In addition to several passports, Ajaj carried manuals on how to construct bombs of the type used in the WTC bombing. But almost nine years later, Ajaj's notebooks and manuals, of which specific pages were submitted as evidence during the WTC trial, have yet to be disseminated to the intelligence community for full translation and exploitation. This information might be vital to analysts' understanding the connections between Ajaj and other terrorists; others in his group; and their intentions, motives, methods of operation, and targets. In part, the problem is a lack of qualified translators within the federal government.

The CIA faces a similar problem with the information it collects overseas, but the agency addresses it with dedicated reports officers located overseas and at headquarters. These officers are responsible for reviewing, prioritizing, and distilling collected information for timely distribution to other elements in the intelligence community and decision-makers concerned with counterterrorism policy. This system allows the CIA to protect sources and methods while disseminating the information as quickly and as broadly as possible.

The commission recommends that the FBI establish its own cadre of reports officers along the lines established by the CIA. The FBI's reports officers should be trained in the information needs of the intelligence community as well as in the legal restrictions that prohibit disclosure of some types of law enforcement information.

### **Cyber-attacks.**

Recent attacks on corporate and government computer networks have demonstrated the potential for damage if terrorists decide to perpetrate a cyber-attack. This is becoming more probable, as hackers and cyber-criminals more frequently target corporate and government IT assets. Developing a vigorous plan for defending against such attacks must become more of a national priority. The commission did not have the time to delve into this issue, but another government commission that is focusing on domestic terrorists will study this problem in depth.

The commission strongly endorsed measures to improve the technological capabilities--in addition to the encryption-related needs mentioned previously--of the National Security Agency (NSA), the FBI, and the CIA. These agencies, particularly the NSA, require an increase in funding to close the technology gaps between them and these techno-terrorists.

International cooperation is essential because cyber-attacks often cross national borders. The commission therefore recommends that the Secretary of State take the lead in drafting and signing an international convention on cybercrime. The main areas covered would be coordination of national laws, better information-sharing mechanisms, avenues for early warning of attacks, and procedures to improve international cooperation in cybercrime investigations. The European Union is now working on a draft of such a convention, and the American government has been involved in these efforts.

### **Counterterrorism**

### **policies.**

On the policy front, the United States needs to pursue counterterrorism efforts against anyone supporting terrorists, including state sponsors, nations that turn a blind eye to terrorist activity, and private individuals and organizations that provide material support to terrorist groups. For instance, some of the state sponsors of terrorism, including Iran and Syria, are in the process of internal change. The United States should communicate to these countries' leaders that it expects changes in their support for terrorism.

*Iran.* In the case of Iran, although the American government hopes that President Mohammad Khatami can institute sensible political and economic reforms, the country continues to be the world's primary state supporter of terrorism. In fact, since Khatami's election, Iranian support for terrorists opposed to peace in the Middle East has actually increased. Furthermore, there is evidence that Iran was involved in the 1996 Khobar Towers barracks bombing in Saudi Arabia that killed 19 American soldiers.

The commission asserted that the American government should make a sustained effort to enlist its allies in pressuring Iran to cooperate in the Khobar Towers investigation. And until there is a definitive

change in the country's support for terrorism, the commission recommends that the U.S. government make no further gestures toward the Iranian government. This suggestion is even more compelling given the evidence produced in the trial of the African embassy bombers, which demonstrated continued Iranian support for attacks conducted by Osama bin Laden on Americans.

*Syria.* It is too early to tell whether the death of Syrian president Hafez Assad will bring any change in that country's long support for terrorism. Syria still allows many terrorist groups to operate openly in Damascus, and a dozen terrorist training camps in the Syrian-controlled Bekaa Valley of Lebanon continue to train terrorists.

The commission recommends that American officials make it clear that Syria cannot expect normal relations with the outside world until it takes concrete, measurable steps to end its support for terrorists. For instance, it should close down the Bekaa Valley training camps and prohibit the resupply of terrorist groups in Syrian-controlled territories. Hopefully, the new Syrian president will see such steps as the prerequisite to obtaining the Western trade and investment essential to modernizing Syria's economy.

The other countries that the American government identifies as state sponsors--Cuba, Iraq, Libya, North Korea, and Sudan--should be made to understand that the United States will continue sanctions until they take concrete steps to cease all support for terrorism. In addition, the Taliban regime in Afghanistan should be designated a state sponsor because it has provided a safe haven to terrorist groups and to fugitives wanted by the U.S. government, such as Osama bin Laden.

There are also states that, while not actively supporting terrorists, turn a blind eye to them. Congress has given the president the power to sanction such nations, but that authority has not been effectively exercised to date. Several countries fall into this category. For example, at times Pakistan has been very helpful in the fight against terrorism. Yet it openly supports a group, Harakat ul-Mujahidin, that has murdered tourists in Kashmir and threatened to kill U.S. citizens.

Sanctions that could be imposed under existing authority include prohibiting military sales to countries that have been designated as "not fully cooperating" with American antiterrorism efforts. Also, the commission recommends that sanctions be broadened to make such countries ineligible for the visa waiver program.

Meanwhile, the commission notes Greece's seeming indifference to the fight against terrorism. Since 1975, terrorists have attacked American citizens and interests in Greece 146 times. All but one of those cases has remained unsolved. And the very week that the commission's report was issued, terrorists struck again with the assassination in Athens of the British defense attaché. No arrests have been made in that case.

### **Nonstate funding.**

As today's terrorist groups receive less monetary support from states, they must seek funding from other sources, such as front organizations, individual sympathizers, and nongovernmental organizations. Thus, it has become increasingly important to disrupt these nonstate funding sources.

Yet America's current strategy against terrorist fund-raising narrowly concentrates on prosecutions for providing material support to designated foreign terrorist organizations (FTOs). Although not impossible to successfully prosecute these cases, it is very difficult to do so under the FTO statute because the prosecution must show exactly where the money went.

Therefore, the commission recommends a broader strategy against terrorist fund-raising in which the U.S. government takes advantage of the full range of legal and administrative powers at its disposal. Money laundering, tax, fraud, and conspiracy statutes all lend themselves to aggressive use against terrorist organizations, their front groups, and supporters. In response to that recommendation, the American government has set up a task force to deal with these issues.

### **The unthinkable.**

According to the FBI, threats involving the use of chemical, biological, radiological, or nuclear weapons in the United States have dramatically increased over the past four years. The potential consequences

of even a small-scale incident are so grave that certain weaknesses in the American approach should be addressed immediately. With the overall objective of establishing controls on biological agents at least as stringent as those applied to critical nuclear materials, the U.S. government should take three concrete steps now to reduce the risk of terrorists obtaining a biological weapon:

- Criminalize unauthorized possession of the worst biological agents.
- Strengthen safeguards against the theft of these agents.
- Control sales of the equipment needed to weaponize biological agents, such as specialized fermenters and aerosol and freeze-drying equipment.

The commission also examined the actions required of the U.S. government in a catastrophic threat or attack and the legal authorities for them. Most of the needed authorities exist but are scattered throughout different federal statutes. Also, there are some gaps in legal authorities, for example, in the quarantine authority of cities and states. Additionally, there is no clear federal authority regarding vaccinations for diseases such as smallpox or anthrax. Finally, it is not clear that federal, state, and local law enforcement officials are aware of their powers for certain types of searches in emergency situations, which vary according to jurisdiction.

As some government officials are not fully aware of the extent of their legal authorities and responsibilities, the possibility exists that in a crisis situation they will be hesitant to act or will act improperly. The commission therefore recommends that the president direct the preparation of a manual outlining existing legal authorities for actions necessary in a catastrophic threat or attack and that the president determine whether additional authorities are needed to deal with catastrophic terrorism.

A central issue is who would be in charge in case of such an event. Many citizens and media outlets have misunderstood one of the commission's recommendations, that "*in extraordinary circumstances*, when a catastrophe is beyond the capabilities of local, state, and other federal agencies, or is directly related to an armed conflict overseas, the president *may* want to designate DoD [the Department of Defense] as a lead federal agency," (emphasis added). An example would be an attack that killed tens of thousands of people.

Effective contingency planning for a catastrophic terrorist attack in the United States—one that could kill thousands of Americans—must include preparation for all plausible contingencies, including the possibility of a federalized National Guard force operating under the direction of the Secretary of Defense. Not to do so would be irresponsible.

In making this recommendation, the commission had in mind the lessons learned in the aftermath of the catastrophic attack on Pearl Harbor, when an executive order signed by President Franklin Roosevelt forced Japanese-Americans to leave their homes, livelihoods, and possessions to live in internment camps. The commission concluded that the best way to minimize threats to civil liberties in such an extraordinary scenario is through careful planning, including a thorough analysis of the relevant laws, the development of appropriate guidelines, and realistic training and exercises. The commission recommends that the National Security Advisor, the Secretary of Defense, and the Attorney General develop detailed plans for this contingency.

To protect U.S. citizens, the nation needs a sustained national strategy in which leaders use first-rate intelligence to direct the full range of measures against terrorists and their supporters. These measures include diplomatic, economic, and commercial pressures; covert action; and military force. As the probability that terrorists will launch mass attacks continues to grow, so do the stakes. Legislation was introduced in fall 2000 that would put into effect almost all of the commission's recommendations. Although the rush to adjourn did not allow a vote in Congress to occur, the commission is hopeful that the new Congress will undertake the creation of a sustained national counterterrorism strategy as a priority matter.

---

*L. Paul Bremer III served as chairman of the National Commission on Terrorism. He is the managing director and senior advisor, political and emerging risks, for Marsh, Inc. He served as ambassador to the Netherlands as well as ambassador-at-large for counterterrorism.*