How to Think About Terrorism

Will better intelligence and technology allow the United States to anticipate future terrorist attacks? History does not offer much reason for optimism, but there are steps we can take now.

BY RICHARD K. BETTS

IN THE AFTERMATH OF SEPTEMBER 11, MANY Americans have embraced the belief, or at least the hope, that acts of terror can be prevented in the future. More-advanced technologies, better-trained people, and better-organized bureaucracies, it is thought, will shield us from danger by revealing the future more clearly than America's intelligence agencies were able to do before the Al Qaeda attacks. This hope goes naturally with the traditional "can-do" ethos of American culture. A little hard thinking shows the expectation to be futile, but a great deal more thought is required if we are to understand what we can reasonably hope to accomplish in combating future terrorism.

If we are ever to turn a clear eye on the threat of terrorism, we must begin by shedding three popular misconceptions: first, that the threat can be ended if we apply more energy, innovation, resources, and talent to counterterrorism, and that the reason for past failures was incompetence or insufficient effort; second, that the maximum effort against all potential attacks that might be mounted inside the United States is either required or possible; and third, that the global war on terror is against terrorism—a tactic—rather than against particular political groups that use the tactic.

To prevent future terror attacks, what is needed above all is good intelligence. Compared with the numbers and strength of the people and institutions they target, terrorists are few and weak, and they are completely vulnerable if identified and located. Since the keys to terrorist success are conspiracy and surprise, the principal way to succeed in counterterrorism is to overcome the enemy's advantage of secrecy. After September 11, many people were outraged to learn that U.S. intelligence agencies had fallen down on the job in "connecting the dots"—that they possessed scattered pieces of information that might have allowed them to anticipate the attack if these pieces had been put together properly. It seemed obvious that if procedures were more careful and personnel more diligent, creative, and responsible, and if the resources applied to tracking potential terrorists were less constrained, disasters could be averted.

That is half true. Stronger efforts naturally raise the odds of success, but much more modestly than people expect.

RICHARD K. BETTS, professor and director of the Saltzman Institute of War and Peace Studies at Columbia University, was a member of the National Commission on Terrorism. Among his books are *Surprise Attack* (1982), *Nuclear Blackmail and Nuclear Balance* (1987), *Soldiers, Statesmen, and Cold War Crises* (1991), *Military Readiness* (1995), and *Paradoxes of Strategic Intelligence* (2003).

Connecting the "dots"—such as this photo of Mohammed Atta and another hijacker boarding a plane in Portland, Maine, on the morning of the September 11 attack—is the unending quest of intelligence services, but history suggests that the task will never be fully achievable.

Contrary to what many assume, the problem is not analogous to minimizing plane crashes or defending against hurricanes. Flying is the safest way to travel because an elaborate system of maintenance and safety measures keeps crashes from occurring more than once in a blue moon. If building better levees had been made as high a priority as airline safety, New Orleans might have been saved from Hurricane Katrina. But counterterrorism is not a fight against nature or a search for flaws that, though perhaps difficult to uncover, are not actively trying to hide. It is a fight against plotters searching for ways to negate or circumvent precautions. Stronger countermeasures can make it harder for them to find those ways, but cannot prevent them from succeeding occasionally if their efforts are strong enough.

Is this view too fatalistic? Unfortunately, the historical record of failure to prevent strategic surprises is overwhelming. In conventional warfare, victims usually misread the evidence or miscalculate their responses, and they can suffer surprise even when their intelligence collection systems and defensive preparations are impressive. This happens for a variety of psychological, political, and organizational reasons. Complex bureaucracies misroute information; the amount of intelligence proves to be excessive rather than insufficient, and salient indicators are buried in a clutter of information; false alarms foster a "cry wolf" syndrome and make victims less sensitive to warning information; uncertainty leads decisionmakers to search for more information, which delays response; enemy deception derails the interpretation of warning data; the victim finds out that an attack is coming, but not where, when, or how it will occur, which hampers response; warnings are disregarded because the indicated attack seems strategically irrational for the enemy, and the evidence is explained away as diplomatic muscle-flexing. And so on. When these cases are scrutinized carefully, it becomes evident that the failures are due more often to normal human limitations and to the skill of the attack's planners than to stupidity or irresponsibility on the part of the victim's officialdom. Organizational changes to fix the problems usually create new vulnerabilities in the process of fixing the old ones.

Hope springs eternal, and of course some measure of improvement is possible. The question is how much we can realistically expect. Inside the Washington Beltway, it has become popular to endorse a "transformation" of the national intelligence system similar to the movement to transform the military forces for the 21st century. The notion that the century requires a whole new approach for a whole new ball game may seem intuitively right, but it is, in fact, wrong. The difference between the world of 2006 and that of 1999 is no more radical than the difference between the worlds of 1999 and 1992. Still, the contrary intuition is psychologically powerful, and when combined with the shock of September 11, it spawned assumptions that major changes in the system would produce major improvements in counterterrorism. The Intelligence Reform and Terrorism Prevention Act of 2004, which mandated the biggest reorganization of America's modern national intelligence structure since its founding in 1947, encouraged the notion that revolutionary change was under way.

THE NOTION THAT the 21st century requires a whole new approach for a whole new ball game may seem intuitively right, but it is, in fact, wrong.

What kind of shakeup *will* do the trick? The impetus for the transformation of the Defense Department has been the prospect of capitalizing on advanced technologies. Can America's comparative advantage in technology overcome deficiencies in intelligence as well? Doubtful. Getting sufficient information on highest-priority threats is harder than it used to be, because technology cannot get at much of what is needed. We can now see that the Cold War after 1960 was, by comparison, a golden age for intelligence collection. Sophisticated reconnaissance satellites and the technology for intercepting and decoding communications could effectively gather most of what was then needed to accomplish the primary missions of American intelligence: locating, counting, and tracking Soviet military forces, and monitoring compliance with arms control agreements.

Against terrorists, the primary mission is to find and track small groups of conspirators in the warrens of teeming cities or in remote mountain hideouts. In such locations, high-tech collection systems are not as useful as on-the-ground reporting from human spies. But though there is agreement all around on the increased importance of such human intelligence, there is no agreement on how to get it when confronting alien cultures and committed enemy support networks in hostile territory. America's minimal success in capturing fugitive Taliban leaders despite our offers of multimillion-dollar rewards is an unpleasant indicator of the difficulty.

With better human sources, more-advanced information technologies, and enhanced organizational coordination, intelligence can be improved and dots can sometimes be connected better than they were before September 11, but the analogy is to raising a batting average 10 or 20 percent, not to making the probability of air crashes minuscule. As long as the threat comes from plotters searching for an opening, the risks of attack will remain substantial. Not all of the risks, however, are of the same gravity, and we must choose those to which we will direct our greatest efforts at prevention.

The number of potential threats is limitless; the resources to combat them are limited. In practice, moreover, we sometimes prefer to keep risks higher than they might otherwise be because we want to keep the benefits we would lose by reducing them. In principle, we say that life is priceless; in practice, we set prices all the time. The most cited example is traffic safety. Americans accept tens of thousands of deaths from auto accidents each year as the cost of convenient transportation. If we wished, we could markedly reduce the number of fatalities by enforcing 45 mph speed limits, requiring all vehicles to have large, resilient bumpers, and establishing 20-year prison sentences for first offenses as a deterrent to drunken driving. But Americans simply do not wish to pay those costs just to save some thousands of lives.

Terrorists have innumerable targets and tactics among which to choose, so the issue for counterterrorism efforts becomes which risks to minimize and which to accept in some measure. The decision is easier for threats at the high and low ends of the spectrum than for those in the middle. In general, terrorist acts that can cause the greatest potential damage should be the first priority for preventive efforts, even if the probability of such acts is low, and those that are very probable but of low consequence should be third in priority. The actions that may occur *between* these extremes pose difficult choices because they are both moderately probable and significantly destructive, and the number of such possible actions that would be costly to counter makes the proper level of effort against them hard to estimate.

Fortunately, many operations that would be the easiest for conspirators to execute offer the least payoff. Assassinations, restaurant bombings, and hostage takings, for example, would horrify the public but would inflict death and damage on a relatively small scale. We might call them acts of "typical" terrorism, of the sort to which European countries adjusted when it occurred episodically in the 1970s and '80s. Americans have not experienced such small blows often enough to take them in stride, but they could probably learn to do so if necessary. To reduce the toll from typical terrorism, we can invest heavily in standard police work, civilian vigilance, immigration controls, and other measures, without undertaking every imaginable draconian precaution—such as forbidding large gatherings of people, encasing restaurant tables in sandbags, or deporting all visitors from Arab countries—that would interfere with other interests.

The terrorists Americans worry most about—Al Qaeda—have not seemed interested in campaigns of frequent, comparatively easy but puny actions. Rather, they appear committed to spectaculars such as the September 11 strikes, which offer a much bigger payoff of shock and awe. Spectaculars, however, are difficult to bring off, especially after September 11. Security crackdowns inside the United States and unrelenting pursuit outside have made it harder for conspirators to gather, catch their breath, and stop looking over their shoulders long enough to develop and implement a complex, coordinated plan.

At the opposite extreme from typical terrorism is the highest-priority category of terrorist threat: the potential use of weapons of mass destruction (WMD) inside the United States, weapons that could kill 10 times or more the number of Americans killed on September 11. The main threats are a nuclear detonation and the effective dissemination of potent biological weapons. Chemical weapons or a radiological "dirty bomb" would be less destructive, but in some circumstances they could still inflict high casualties or contaminate areas, with psychological effects greater than the material damage.

Attacks as spectacular as these are also the least likely. Building nuclear weapons from scratch is a process of greater complexity than folklore suggests, and probably well beyond the capacity of the Qaeda network. The greatest dangers at present are the theft of ready-made weapons from inadequately secured stockpiles in Russia or Pakistan and the sale of fissionable material by North Korea. Barriers against the effective use of biological weapons are lower than those against the use of nuclear weapons, but still high. Despite the popular notion that it is easy to whip up biological weapons in a bathtub, refining them for efficient dissemination that could infect tens of thousands of people requires exceptional skill and technology, and secure working areas. Though they would be difficult, such projects are clearly possible, and terrorist groups with the resources and organization, high motivation, and an undetected base of operations may well succeed eventually in deploying biological weapons. Under optimal operational conditions, the most potent biological agents would have as much killing capacity as normal first-generation nuclear weapons.

An effective WMD attack would be so devastating that this category of threat warrants maximum attention. To reduce the chances that terrorists can acquire or transport WMD, much has been done—through investment, for example, in detection mechanisms, the better tracking of dangerous materials, and the inspection of cargo coming into the country. To maximize the odds of prevention, however, efforts could go further, and tradeoffs with other interests should be made more readily than they are in regard to low-threat typical terrorism. As veteran strategist and policymaker Fred Iklé wrote in *The Wall Street Journal* (Aug. 5, 2005), "To send a man to Mars we have a generously funded, well-integrated project; but to detect a smuggled nuclear bomb on its way to a U.S. city we allocate a puny fraction of those funds and scatter it among a multitude of disjointed studies that feed congressional pork."

Scenarios for catastrophic WMD attacks range from tens of thousands of fatalities to hundreds of thousands, especially if multiple strikes are coordinated, as they were on September 11. More probable—because the technical obstacles are fewer—are attacks that are less awesome in their effects but still much worse than the typical terrorist incident that causes, say, 50 casualties. Some middle-range possibilities pose hard choices because the costs of minimizing the risk are higher than they are for coping with typical terrorism, while the benefits are less clearly compelling than the benefits of preventing a mushroom cloud over Capitol Hill.

One middle-range example would be a set of strikes against airliners in flight by teams of terrorists with shoulder-fired anti-aircraft missiles, or MANPADS (man-portable air defense systems). Counterterrorism experts have long known that such weapons exist in large numbers around the world, and that Al Qaeda or its ilk might obtain them. For various technical reasons it would not be easy for terrorists to deploy those weapons effectively, and the probability of a successful coordinated strike that knocks down four or five 747s simultaneously is low—almost as low, perhaps, as the probability of what happened on September 11. Nevertheless, if such an event occurred tomorrow morning, no counterterrorism expert could claim to be surprised. How would political spinmeisters word tomorrow afternoon's government press release to explain why every effort had not been made to prevent this type of attack?

Well, the statement might note that much has in fact been done to counter such a threat—efforts, for example, to find and buy or neutralize loose MANPADS, to institute the surveillance and patrolling of approaches to airport runways, and to develop antimissile systems for civilian aircraft. But how to explain why the onboard antimissile defenses that are already available—such as flare and laser systems—have not yet been installed (though the president's own plane has such a system)?

One reason is the expense. According to a 2005 RAND Corporation report (*Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat*, by James Chow and others), it would cost $11 billion to equip U.S. airlines with antimissile systems and more than $2 billion annually to maintain and operate them, while the total federal budget for transportation security is well under $5 billion. Another reason is that existing defensive systems are not optimally designed, and better technologies are in the works. Why invest now? Further, the available antimissile systems could have dangerous side effects if they were used, such as fires started by flares or people on the ground blinded by lasers. All of these may be reasonable grounds for delay in maximizing countermeasures against the potential MANPADS threat, given their dubious benefits and other demands on funds. But would the public understand why the hard choice had been made *not* to do everything possible?

One nightmare of counterterrorism specialists is the large supply of shoulder-fired anti-aircraft missiles potentially available to terrorists. Yet it may make sense not to do everything possible to defend against them.

Another hypothetical terrorist act would be the effective dissemination of aerosolized anthrax in several American cities on the same day, which might not kill huge numbers—since a good public-health response might save most infected people with antibiotics—but might nonetheless overwhelm response capabilities in some areas, exhaust stockpiles for treatment, and cause several thousand fatalities. In the days after such a disaster, the government would be called on to explain why it had not mounted a crash program to overcome the obstacles to mass vaccination against anthrax. These obstacles have been significant: the unsatisfactory quality of available vaccines, inadequate production facilities, cumbersome requirements to repeat vaccinations to keep protection active, negative effects on the health of some portion of those vaccinated, and more. But on the day after, would the public understand that hard choice?

As long as threats such as these are hypothetical, potentially numerous, less than monumentally catastrophic, and expensive to counter, the risks, of both their occurrence and their potential consequences, will be left higher than they could be. And as long as the threats do not become reality, these judgments will seem prudent. The morning after one of them *does* become real, the choices will be discredited. The way out of this dilemma is not obvious. Its very intractability highlights the point that people should think of the war on terror as being like the war on crime—a struggle in which success is measured not by final victory but by declines in the incidence and seriousness of attacks.

Terrorism is not an enemy. It is a tactic used by an enemy in pursuit of a political objective. There will be no final victory against terrorism, but there may be victories that are close enough to final against particular political groups that use terror tactics. Italy's Red Brigades, Peru's Sendero Luminoso, Mozambique's Renamo, and America's Ku Klux Klan may not be extinct, but we do not worry much about them anymore. Victories, such as they are, usually result from a combination of forcible attrition and an evolution in the political contexts and social environments of these movements that reduces sympathy for their agendas. Effective counterterrorism thus needs to begin with an understanding of the political motives and incentives of terrorists and, where possible, with the ability to dampen them.

Understanding radical groups in other cultures is difficult. Insight requires a degree of empathy, and parochial observers find it hard to empathize with different worldviews, while cosmopolitan observers naturally find reactionary ideologies alien and unfathomable. It is also vital to distinguish between empathy and sympathy. Anyone who appears to sympathize with terrorists will be discredited as a source of wisdom on counterterrorism, but those who do not empathize with terrorists will not get far enough inside their heads to develop the maximum base of intelligence for counterterrorism.

Americans need not worry much about understanding terrorists who do not threaten us, such as the Tamil Tigers, the Irish Republican Army, or Colombian drug lords. But they must deal head-on with the problem of understanding the main group at which American counterterrorism efforts are now directed: Al Qaeda. Most normal Americans find it impossible to empathize with any movement that uses suicide bombers to kill large numbers of civilians, especially American civilians, because empathy requires admitting that somewhere in the world intelligent people regard U.S. policy as aggressive, oppressive, and murderous.

The prevalent urges to attack the "root causes" of terrorism are generally misguided and unconvincing, because they cite generic problems, such as poverty, religious fanaticism, or poor education, that exist in far more places than the few that spawn terrorists. If, however, we think of the root causes as the specific political grievances of the groups in question, the urge to focus on them is a good one. Confronting the enemy's political agenda will clarify just how much U.S. policy can or cannot do to reduce the incentives to use terror against our society, and determine whether counterterrorism has to rely on force alone to suppress the terrorist actions that flow from those incentives.

This does not mean that we should meet terrorist demands, but rather that *knowing* the enemy better increases the odds of finding an opening in his armor, or of figuring out better ways to use propaganda (what "public diplomacy" for the war on terror really means) to sway the populations whose allegiance is at issue. Dealing with future terrorism will require plenty of inventive intelligence activities, to be sure, but there will be no single technological or bureaucratic fix on which to pin all our hopes. Counterterrorism will require a lot of plain old politics and psychology. ■