3 Assessing the Terrorist Threat

> One fact dominates all homeland security threat assessments: terrorists are strategic actors. They choose their targets deliberately based on the weaknesses they observe in our defenses and our preparedness. We must defend ourselves against a wide range of means and methods of attack. Our enemies are working to obtain chemical, biological, radiological, and nuclear weapons for the purpose of wreaking unprecedented damage on America. Terrorists continue to employ conventional means of attack, while at the same time gaining expertise in less traditional means, such as cyber attacks. Our society presents an almost infinite array of potential targets that can be attacked through a variety of methods.
>
> —Executive Summary, President's National
> Strategy for Homeland Security (July 2002)

While terrorists' objectives may be uniform in that they tend to center on altering a government or changing its policy, the methods for carrying out the attacks designed to achieve these objectives can be as varied as the attacker's imagination allows. Thus, unpredictability is a key tool in the terrorist arsenal that boosts the chances of an attack being a success.

For instance, viewing only al Qaeda–backed attacks on U.S. interests during the past decade, we see that the first three targets were hit by trucks carrying heavy, conventional explosives: in 1993, the WTC in New York City; in 1996, the American troop barracks at Khobar Towers in Riyadh, Saudi Arabia; and in 1998, U.S. Embassies in Nairobi, Kenya, and Dar es Salem, Tanzania. Thus, while al Qaeda had achieved unpredictability in regard to the locale of its attacks (both inside and outside the United States) and the targets (business interests, military personnel, and government offices), it had failed to achieve unpredictability in regard to the method of delivery.

This changed, perhaps as al Qaeda matured, with the attack on the American Aegis-class destroyer USS *Cole* in 2000. As the ship entered the Port of Aden in Yemen for a routine stop, it was approached by a small anchoring skiff in a normal fashion. However, this skiff was guided by two terrorists and was loaded with high explosives designed to breach the reinforced steel hull of the warship. This, of course, is what happened. Then, in 2001, the method of delivery was changed yet again by resorting to hijacked, fuel-laden aircraft in the September 11 attacks that jolted the psychology of our country so profoundly.[1]

Consequently, al Qaeda eventually achieved the desired level of unpredictability in regard to delivery. Of secondary significance is the fact that not all of the attacks culminated in their desired outcome (the WTC did not collapse in 1993 and the USS *Cole* did not sink in 2000). However, government officials must now worry not only about where such attacks will occur and at what institutions they will be directed but also what avenues of delivery are open and potentially available for use. The possibilities are many, and the remedial countermeasures are both few and impracticable.

After the first WTC attack, followed by the 1994 truck-bomb explosion that decimated the Alfred P. Murrah Federal Building in Oklahoma City and the subsequent al Qaeda truck bombs, federal and military installations were ringed with concrete barricades and Pennsylvania Avenue in front of the White House was shut down and cordoned off from vehicular use. Physically limiting the proximity of ships and airplanes in a similar fashion is virtually impossible.

With regard to sea traffic, about 6 million containers arrive via ship at U.S. seaports every year, sometimes averaging over two thousand cargo containers each hour. These are taken by barge upriver or loaded onto semi-trucks or trains and then transshipped overland to their ultimate destination, be it Dallas, Salt Lake City, Atlanta, or Omaha. About 90 percent of world trade flows along international sea lanes and is carried on such cargo ships. Only 2 percent of containers arriving in the United States are checked by federal agents. It is a random sampling intended to meet the goals of fulfilling U.S. security interests and keeping would-be terrorists off-guard while not slowing down the shipping process to the point that it would harm our economy.[2]

By any measure, this process does not fulfill the first two goals but does fulfill the third. However, there are no easy solutions. We do not have the equipment to X-ray all containers entering our ports, nor do we have the financial or physical capacity to build, deploy, and operate them. And the U.S. Coast Guard, tasked with securing our country's waters, has neither the manpower, training, nor equipment to accomplish the task. As this excerpt from the *New York Times* explains, their efforts have been rewarded only with failure:

> Shortly after September 11, the Coast Guard began a program that requires every commercial ship destined for the United States to send authorities a list of crew members' names 96 hours before docking, so that they can determine if there are terrorists on board. . . . [T]he Coast Guard receives several thousand names a day. But it has no way to know whether a given name is the true identity of a crew member, or an invented one. Further, most names are sent by fax, on sheets that are frequently illegible or with notations in languages that officials cannot read.
>
> Then, because of lack of coordination among databases, the Coast Guard has no access to the most important criminal and immigrant computer files, and must rely on other agencies to run the checks on the names. . . . But even if a suspicious ship is identified, the Coast Guard crews that search it have no training to identify terrorists or their equipment, and no sensors or related detection devices that can locate chemical, nuclear or other weapons. . . . [And] as a matter of policy, the Coast Guard does not ordinarily even board container ships, since there is no way to inspect the contents of the containers [which] are often stacked six-deep and -wide, and so gaining access to many of them is impossible until they are unloaded, even though containers that may hold terrorists or weapons of mass destruction are a central concern in Washington.[3]

With regard to air traffic, emphasis has been placed on identifying and apprehending terrorists before they strike, with more serious measures implemented once the plane is airborne.

Preflight: Airport security is now regulated by government oversight, and the level of passenger scrutiny has increased markedly while the level of baggage scrutiny has increased only slightly. But the new federal agency tasked with stepping up preflight airport security, the Transportation Security Administration (TSA), has failed spectacularly in its mission. None of the congressional deadlines for action were met.

As of midsummer 2002, of the sixty-three thousand federal airport screeners needed, only three thousand had been hired, and of the 429 major airports that were to be staffed with such screeners by Thanksgiving, only three were so outfitted. And while bag-matching policies are in effect for checked luggage at all airlines now, the agency was unable to provide bomb detection machines to physically screen such luggage. In fact, most of the money earmarked for this project was instead spent on "highly paid consultants and lawyers" who were hired to advise the agency on how to meet its December 31, 2002, deadline for deploying these devices.[4]

Nor has any progress been made to date on screening air cargo containers that piggyback along with U.S. mail on passenger jets and make up 40 percent of domestic cargo in America. Thus, potential suicide terrorists can still check a bag with a time-delayed bomb and board a plane (under the current bag-matching scheme) or gain access to an air cargo container. The TSA's failure to meet any of its legislative mandates had become so apparent by the summer of 2002 that the administrator was fired and replaced with a former navy admiral.[5]

In-flight: Pilots have been issued stun guns, cockpit doors have been locked, and all flights approaching Reagan National Airport in Washington, D.C., now require passengers to remain seated thirty minutes prior to landing or the plane will detour to another airport. The debate continues on issuance of pistols to cockpit crew. On the one hand, the enhanced security offered by armed pilots cannot be denied. On the other, once a gun is fired, a missed shot could puncture a window, causing the entire cabin to depressurize at a potentially lethal altitude, resulting in the crash of another passenger jet.

Landing: President Bush has issued an order for military fighters to shoot down any suspicious, nonresponsive passenger aircraft veering off its intended flight path. For several months after September 11, F-15 and F-16 fighter jets circled the skies over most major U.S. cities, supported by refueling aircraft. These patrols were scaled back significantly in the spring of 2002. They now only operate sporadically and in a random sequence. Thus, a nonresponsive passenger jet would have to either deviate or be identified early enough in its landing pattern to allow fighters time to scramble and intercept the jet.

With regard to the attack method not yet employed by an al Qaeda group—rail—scant attention has been paid to intercity passenger or cargo lines. Most concern has centered instead on intracity subway systems, which are inherently more manageable and arguably more threatening. However, a weapon correctly placed and timed on a train entering Chicago, Philadelphia, or Washington's Union Stations; New York's Grand Central or Penn Stations; or the Amtrak stop next to Baltimore's Camden Yards baseball park could be just as destructive. Because the security focus is shifting to known transport delivery methods such as air and trucking, rail may present an easy opportunity for a group like al Qaeda to exploit in its endeavor to remain unpredictable.

This chapter focuses on the emerging terrorist threats faced by America. The threats exist both internally—from domestic sources—and externally—from foreign sources. They are not limited by geography, only capability. The traditional threats are so defined by their common usage of conventional high explosives. Systemic threats are characterized by their use of weapons of mass destruction (WMD) that often entail ripple effects beyond introduction. These include nuclear, biological, and chemical modalities of attack. Cyberthreats refer to electronic attack and/or theft via Internet, intranet, or other method. Al Qaeda's continued viability to threaten the United States and American interests abroad is also examined.

Guarding against Traditional Threats

Traditional sorts of terrorism take many forms: hijacking, kidnapping, hostage taking, ransoming, murder, and property damage. They typically also involve a conspiracy of some degree. These acts are sometimes carried out at gunpoint, but more often they occur under the threat of explosive detonation. The logic of this is fairly simple and straightforward. If one's destructive capacity is increased exponentially, then so is one's influence and thereby one's ability to coerce. Hostages are often a necessary evil in order to protect the terrorist from a military reprisal, preemptive strike, or sniper's bullet before he realizes his objective. Murder of some hostages is also deemed necessary, according to the internal logic of the terrorist mind, to demonstrate the seriousness of his intent.

Governments around the world deal with hundreds of internal and external traditional terrorist threats and attacks each year. Many of these are tied to political goals such as greater autonomy within a governing federation or outright independence from a larger state. Examples include the struggle of the Chechens in Russia, Uigirs in China, Basques in Spain, Corsicans in France, Tamils in Sri Lanka, Palestinians in Israeli-controlled territories, and Kurds in Turkey. However, other similarly violent struggles, such as that of the Irish Republican Army in the United Kingdom and the indigenous Zappatistas in southern Mexico, have been overcome through third-party overture leading to peaceful political compromise. Thus, the possibility of compromise and cessation of violence is possible if it is genuinely in the interest of both sides to engage—although political reality may dictate otherwise.

According to the U.S. Department of State, there were approximately 125 separate significant terrorist incidents around the world in 2001. *Significant* is officially defined as resulting in "loss of life or serious bodily injury to persons, abduction by kidnapping, major property damage, and/or is an act or attempted act that could reasonably be expected to create the conditions noted."[6]

Americans are not used to thinking of themselves as ready targets in the global occurrence of terrorism. Terrorist attacks statistically do not occur in North America as often as in other countries on other continents. Perhaps this is a reflection of our society; perhaps it is a reflection of our physical distance across the Atlantic, Pacific, and Caribbean from the rest of the world. Whatever the reason, the quintessential, perhaps innocent, American psyche tends to relegate images of mass death and wanton destruction confronted by it on the nightly news, Internet, or newspaper to faraway places locked in complicated cycles of conflict that are not the concern of suburban households in Cleveland or Peoria. At most, America's interests, offices, and institutions in other parts of the world have been at risk as targets of terrorism, but not Americans themselves here in the homeland.

Comparatively, until 9/11, the United States had not suffered the scourge of international terrorism to the degree the rest of the world had. Apart from the 1993 WTC attack (which was basically a failure) and the random shooting of a Danish national atop the Empire State Building in 1997, the worst terrorist act suffered by America at home in that decade was McVeigh's destruction of the federal building—an act of domestic, not international, terrorism.

This notion of immunity from foreign attack at home is buttressed by our historical experience. The terrorist acts that culminated in the destruction of the WTC and the severe damage of the Pentagon on September 11 together constituted the first major attack by a foreign entity suffered by the United States at home since Pearl Harbor in 1941 and the first in the continental United States since the British burned Washington, D.C., in 1814. All of the major wars fought by America since the end of the Civil War in 1865 have been overseas. The big problems of the twentieth century were not guarding against attack or military invasion during the cold war—which was waged by proxy abroad—but fighting domestic crime and drug addiction. However, this notion began to erode in the past decade.

The 1993 truck-bomb attack on the WTC startled us and caused us to begin thinking about our vulnerabilities at home. But Ramzi Yousef's cryptic remark to the FBI that they would return to finish the job was disregarded. Timothy McVeigh's detonation of a very simply constructed, very large fertilizer-based truck bomb in 1994, which killed 168 people in Oklahoma City, jolted us again and caused Americans to ask how such a horrible terrorist act could be perpetrated from within. The combined attacks on September 11 by Osama bin Laden's al Qaeda network—which turned four jet aircraft into human-guided missiles that killed approximately twenty-eight hundred people in three states, collapsed the WTC, and damaged the Pentagon—utterly shattered the widely held latent idea that we were immune on our continent from international terrorism.

Slowly, we in the West are starting to realize that the process of globalization (i.e., the further integration of networking capability) is a weakness as well as a strength. On the one hand, these networks provide a boost to supercharge our economies, greasing the wheels of commerce. On the other, they can be utilized by terrorists. For example, the 9/11 hijackers availed themselves of the streamlined air transit network, bin Laden spread his poisonous message to inflame anti-American passions through the television media, and the anthrax attacker who unleashed his or her deadly spores in October 2001 utilized the postal network to spread biological agents.

Highway systems, railroads, cyberspace—almost any conceivable network, be it digital, physical, or media, is susceptible to abuse by terrorists. As Yale historian John Lewis Gaddis observes:

> [I]t was held to be a good thing that capital, commodities, ideas and people could move freely across boundaries. There was little talk, though, of an alternate possibility: that danger might move just as freely. . . . It was as if we had convinced ourselves that the new world of global communications had somehow transformed the old aspect of human nature, which is the tendency to harbor grievances and sometimes act upon them.[7]

And so the question becomes, How do we guard against such attacks in the future? First, there is the physical response. Short of closing the border and cutting off the benefits of globalization, we can attempt to keep terrorism at bay through heightened awareness, security, screening, and covert intelligence. There is also the nonphysical response. This entails changing the mind-set of those who would do us harm or at least altering the equation by eliminating the latent urge in the hearts of those who can be inflamed and exploited by the clever few in pursuit of their evil ends.

Heightened Physical Security

As both the government and the public, through the news media, engaged in an appropriate and thoughtful retrospective on the events of 9/11 in the spring and summer of 2002, the myth that the federal government works as a single interlocking mechanism was laid bare. The Immigration and Naturalization Service (INS) was still processing visas of some of the hijackers and approving flight school applications. The FBI had detained Zacarias Moussaoui in Minneapolis, where he was attempting to engage in flight instruction, while an agent in Phoenix had penned a memo theorizing an attack by aircraft on the WTC that was stopped before making it up the chain of command to Washington. The CIA had been monitoring two of the hijackers for several months in Malaysia and elsewhere, following them into the United States, but did not share its information with any other federal office after losing track of them.

The problem—the reason that the 9/11 attack slipped though the cracks—is largely interinstitutional. The current system of ensuring the country's physical security sufficiently to counter a terrorist threat belies its historical piecemeal construction—the ad hoc creation of agencies with limited powers to address specific and unrelated issues. Just as it is no surprise that parts of a machine not designed to work together often fail to keep the machine running, it should come as no surprise that confusing and inconsistent interactions among the CIA, FBI, National Security Agency (NSA), Bureau of Alcohol, Tobacco, and Firearms (ATF), Drug Enforcement Administration (DEA), Defense Intelligence Agency (DIA), INS, and myriad other instrumentalities can fail to effectuate a reliable bulwark against emerging terrorist threats.

Consequently, while the government as a collective entity had several pieces of the puzzle that could conceivably have led to shutting down the 9/11 conspiracy before it went into effect, the elements of timing, nonexistence of a meaningful information-sharing system, and inability to bring the pieces together in one office worked against the puzzle ever being completed. These revelations were disturbing, even prompting the *Wall Street Journal* to call for FBI director Robert Mueller's resignation. However, they are certainly not startling.

The INS's rigid strategy of methodically handling the overwhelming workload of visa tracking, naturalization, illegal immigrant roundup, and deportation in a nonresponsive manner practically precluded the civil servants in that agency from any creative thought process. Moreover, intelligence sharing is anathema to the cultures of the CIA and FBI, both of whom enjoyed complete primacy and unquestioned power within their spheres during the cold war. Potential leaks were plugged from within and classified data jealously guarded against Soviet compromise. After the cold war, in the 1990s, both agencies were rocked by scandal and perceptions of ineptitude that seriously damaged their ability to meet their mandates while simultaneously reinforcing a defensive "bunker down" posture that made the likelihood of information sharing even less likely.

The CIA ensures America's security while operating abroad. However, its foreign and international operations were scaled back and human intelligence-gathering capacity limited in favor of technical advances in satellite capabilities. Thus, the agency was inaccurate in its assessment of the Soviet Union's ability to perpetuate itself beyond 1991 and completely failed to detect testing of nuclear devices by India and Pakistan in 1995. These errors together with the exposure of moles and double agents within the CIA caused Congress to publicly question the agency's continuing mission.

The FBI is the CIA's equivalent at home and much more. Its law enforcement arm is the most widely respected in the world. However, the FBI's own difficulties were highlighted in the 1990s by the public discovery of its own internal moles, such as Robert Hanson, together with a series of unpopular high-profile cases such as the Ruby Ridge fiasco and the Waco conflagration. However, the real weakness of the FBI—its internal culture of suspicion, secrecy, and rigidity—was not fully exposed until the September 11 attacks.

The NSA, an organization created after World War II specifically to avert another Pearl Harbor–type surprise with a $7 billion budget (twice that of the CIA), is charged with enhancing American security through electronic eavesdropping and code breaking. But its failures in this regard have been both ironic and flagrant. Of the 6,500 languages spoken around the world, this agency, which is supposed to be the center of communications sophistication, only has linguists trained in 115 of them. On September 10, 2001, the NSA intercepted conversations from Afghanistan, at least one of which was from an al Qaeda operative referring to September 11 as the "big match" and calling that day "zero hour." These messages were not translated until September 12. Moreover, the al Qaeda cell that hijacked American Airlines flight 77 from Dulles International Airport lived just blocks away from NSA headquarters in Laurel, Maryland. As the *Washington Post* put it, while "the terrorists pulled out of the Valencia Motel on Route 1 on their way to Dulles . . . they crossed paths with many of the electronic spies who were turning into Fort Meade, home of the NSA, to begin another day hunting for terrorists."[8]

In a July 2002 report to the Speaker of the House, the Permanent Select Committee on Intelligence's Subcommittee on Terrorism and Homeland Security noted that one of the common crippling weaknesses shared by the CIA, FBI, and NSA was a critical lack of Arab-speaking agents. Because of this, a backlog of documents and interceptions thousands of files deep went unanalyzed. Moreover, the NSA's technology had not developed to the point that it could track a suspect globally—only sporadically.[9]

In response to these failures, the government began retooling each of these agencies. The intent was to generate greater interaction between the FBI and CIA, to redefine the FBI's mandate, to streamline the INS's processing capability and integrate passport/customs control and border security, and to change the NSA's mission from passive information gathering to proactive targeting and hunting. However, government policymakers, especially in the DOJ, received a fair amount of criticism warning them of encroaching too much into areas of civil liberty that the public holds dear. Balancing its mission to protect Americans evenly against their legally guaranteed freedoms became the daunting and unenviable challenge.

Many of the bureaucratic and institutional reforms undertaken by the separate agencies were significant ones, such as allowing the CIA to have operational control of Hellfire missiles in the field for the first time and easing the Church Committee restrictions on it in relation to surveillance and assassinations.[10] But those undertaken by the FBI were both dramatic and public. In testimony before the House Appropriations Committee's Subcommittee for Justice and Related Agencies, FBI director Mueller explained how he has redirected that agency's mission toward focusing on counterterrorism efforts. Specifically, this entails a ten-point priority list that the director believes will put the FBI on track to fulfilling its new role:

1. Protect the United States from terrorist attack.
2. Protect the United States against foreign intelligence operations and espionage.

3. Protect the United States against cyber-based attacks and high-tech crimes.
4. Combat public corruption at all levels.
5. Protect civil rights.
6. Combat transnational and national criminal organizations and enterprises.
7. Combat major white-collar crime.
8. Combat significant violent crime.
9. Support federal, state, municipal, and international partners.
10. Upgrade technology to successfully perform the FBI's mission.

The rank order of this list reflects the new priority placed on protection, especially with regard to the first three items. This effectively puts the agency in the business of anticipation and prevention rather than evidence collection for future prosecution—its prior focus. To back up this realignment, Director Mueller has reallocated significant manpower within the FBI. He has ordered a permanent shift of 518 agents from criminal investigation to counterterrorism duty. Fully 400 agents will be removed from drug investigations to join 59 taken from white-collar crimes and another 59 from violent crimes. These new recruits in the FBI's own war on terror will be distributed directly to counterterrorism (480), security (13), and training of new special agents at Quantico (25).[11]

The FBI, under DOJ cover, has also executively increased its powers of surveillance—dropping the old standard trigger, based on "information or an allegation whose responsible handling required some further inquiry" (which did not even constitute probable cause), entirely. This move itself triggered a justified, albeit scathing, reproach from William Safire in the *New York Times:*

> Under the police powers it operated under last year, and with the lawful cooperation of a better-managed CIA, an efficiently run FBI might well have prevented the catastrophe of Sept. 11. . . . To fabricate an alibi for his nonfeasance, and to cover up his department's embarrassing cut of the counterterrorism budget last year, Attorney General Ashcroft—working with

> his hand-picked aide, FBI Director "J. Edgar" Mueller III—has gutted guidelines put in place a generation ago to prevent the abuse of power by the federal government.
>
> They have done this deed by executive fiat: no public discussion, no Congressional action, no judicial guidance. If we had only had these new powers last year, goes their posterior-covering pretense, we could have stopped terrorism cold. Not so. They had the power to collect the intelligence, but lacked the intellect to analyze the data the agencies collected. . . . Thus we see the seizure of new powers of surveillance is a smokescreen to hide failure to use the old power.
>
> . . . [U]nder the new Ashcroft-Mueller diktat, [the] necessary hint of potential criminal activity is swept away. With not a scintilla of evidence of a crime being committed, the feds will be able to run full investigations for one year. That's aimed at generating suspicion of criminal conduct—the very definition of a "fishing expedition."[12]

The White House has not been immune from institutional redirection either. Immediately in the wake of September 11, President Bush created the executive Office of Homeland Security, headed by former Pennsylvania governor Tom Ridge, to coordinate the efforts of the nation's dispersed and divergent federal security agencies, offices, and suboffices. Given the amorphous nature of this new office, its limited budget, and unclear jurisdiction, the degree of its effectiveness during the ensuing months was seen as problematic. The most tangible item to emerge from the office was a color-coded terrorist threat system running from green to red. Beyond this, the new presidential advisor has had closed meetings in the White House, the subjects and contents of which are denied to the public. Ridge, an advisor unapproved by Congress, like the chief economic advisor and the national security advisor, is not amenable to answering questions from congressional committees.[13]

Partly in response to congressional criticism of the Office of Homeland Security's progress, secrecy, and unamenability to oversight and partly in an effort to sew together the overlapping intelligence analysis functions of various separate agencies and the homeland security functions of others in a seamless institutional framework that is both responsive and flexible, the Bush administration proposed the creation of a new cabinet-level Department of Homeland Security.

Legislatively, Congress acted on President Bush's recommendation to create this new department, which will be separate from the Office of Homeland Security and which is envisioned as essentially an amalgam of intelligence and threat-analysis divisions from the CIA, FBI, and other agencies brought under one administrative roof while leaving the intelligence-gathering apparatus in place at those agencies. The legislation bringing this federal entity into being will be discussed in chapter 5.

The legislative branch is not wholly unconcerned about its own skin. Former Speakers Tomas Foley (D-Washington) and Newt Gingrich (R-Georgia) have suggested reforming the House of Representatives' rules for replacement of members in the event of a catastrophic attack against Congress to ensure continuity of that body:

> The executive branch has recognized just how real the danger is and has taken precautions. . . . In addition to the vice president's moving to a separate, secure location in periods of high threat . . . scores of other senior officials are on rotating assignments outside of Washington. . . . The legislative branch must take similar precautions. . . . [While] the Constitution permits governors to appoint interim senators to serve until the next election . . . each vacancy in the House . . . requires a special election. . . . [I]n recent cases, it has taken an average of 117 days to fill a vacancy. . . .
>
> The expeditious path is for the House immediately to adopt a change in its rules authorizing each member to pre-designate an interim successor who could serve for the period between catastrophic loss of House members and the election of successors. The Constitution explicitly provides that the House shall make its own rules concerning its members and shall be the judge of its members' qualification.[14]

Finally, the secretary of defense is considering the use of Special Operations Forces as hit squads to be dispatched around the globe eliminating al Qaeda operatives, disrupting terrorist activities, and foiling plots to target American interests. Delta Force and the Navy SEALS are the most likely groups to be tapped for such missions. If approved, these military units would find themselves executing many of the tasks formerly in the bailiwick of the CIA. The argument in favor of such a move is very persuasive—increasing our ability to respond creatively and quickly in a military capacity to an unpredictable opponent. However, the most troubling aspect of this idea is that the military would be able to operate clandestinely, unchecked by political or legal constraints.

Traditionally, the foreign operations by the CIA involving lethal force have been undertaken with the imprimatur of a secret finding by the president that is then monitored by closed select intelligence committees of Congress. Special Operations missions would not be subject to similar control. The covert operations under consideration at the Pentagon would involve these units in longer-term missions in countries where the United States is not currently engaged in open armed conflict and where the governments are not necessarily informed of their presence.[15]

Clearly the wisdom of employing such plans lies with executive discretion. But the possibility of doing so without the same legal constraints placed on the CIA is disturbing and goes against the grain of checking executive power. The balance in this case tips more in favor of creating conditions ripe for abuse of power. In a representative democracy, the citizens cannot simply trust the executive to do the right thing. For the system to work, the decision-making apparatus must be participatory, not exclusive and paternalistic.

Outreach to Alter Perceptions

There is some debate about why the September 11 attacks, and other al Qaeda strikes against the United States, happened. The conventional response domestically from the administration on down has been that these groups hate us and oppose what we, as Americans, stand for in the world. The alternate response dismisses this as a Western-centric point of view and, instead, this response holds that the attacks stem from strife within Islam itself about the future of that religion and its believers. The following extract from a review of Princeton professor Michael Doran’s essay “Somebody Else’s Civil War” encapsulates that view:

> [T]he United States has been sucked into a struggle within the Muslim world. This battle pits those, such as bin Laden, who seek to re-create the era when the Prophet Muhammad ruled the Islamic lands, against those who actually govern Muslim countries today. Bin Laden used Afghanistan as a base to launch a jihad across the Muslim world, hoping thereby to bring "apostate" regimes such as Saudi Arabia within the fold of true Islam and restore the caliphate from Spain to Indonesia. By this view, the attacks on the World Trade Center and the Pentagon were collateral damage in a struggle for the hearts and minds of the *umma*—the worldwide community of Muslim believers. . . . [B]in Laden hoped that the attacks against the United States would spark uprisings by Muslims against their own American-backed regimes. As Sandy Berger [former National Security Advisor in the Clinton Administration] observes in his own essay, "bin Laden's ultimate twin towers are Pakistan and Saudi Arabia."[16]

If this is true, then bin Laden's gambit has certainly failed, at least in the short term. No such fundamentalist Islamic revolution has swept the Muslim world since 2001. However, if the terrorist threat to the United States does stem from an irrational hatred of our culture, politics, worldview, economic policies, or any other manifestation of who we are as a people, then this hatred must be addressed as part of the administration's response.

Over the ensuing weeks following the September 11 attacks, newspapers across the country began to ask, "Why do they hate us?"[17] If hatred of the West or of America in particular is indeed part of the underlying rationale supporting the efforts of al Qaeda, then in order to articulate a meaningful response, we must struggle to understand the genesis of the hatred harbored against our hegemony.

What America did to deserve such unbridled animosity is unclear. Apparently, Osama bin Laden and his colleagues were incensed about America's involvement in the Middle East on a variety of points, which led to a general amalgam of single-minded abhorrence fused with indignancy. But political hatred alone was not enough to inspire suicide terrorism; religious fervor had to be tapped. As Professor Fouad Ajami of Johns Hopkins University's

School of Advanced International Studies notes, bin Laden has managed to tap into religious zeal for political purposes:

> A sacred realm apart, Arabia had been overrun by Americans, bin Laden said. "For more than seven years the United States has been occupying the lands of Islam in the holiest of territories, Arabia, plundering its riches, overwhelming its rulers, humiliating its people, threatening its neighbors, and using its peninsula as a spearhead to fight the neighboring Islamic peoples." Xenophobia of a murderous kind had been dressed up in religious garb.[18]

Still, we must understand that these grievances change character as they are viewed through the fundamentalist lens, as presented by people like bin Laden.[19] For instance, traditional U.S. support of Israel translates into lack of sympathy for the Palestinian cause. The American-led Gulf War, intended to ensure political and economic stability in the region, translates into the dressing down of an Arab leader who presumed to defy the West. The presence of U.S. troops in Saudi Arabia for security purposes after 1991 translates into two things: reliance by the corrupt House of Saud on hired foreign mercenaries to retain power and Western assurance of continued, uninterrupted oil flow with no regard for the Arab people. Approval of American military actions abroad by the UN Security Council translates into further revelation of that body as a willing tool of American foreign policy.

How do we affect these incorrect perceptions that provide a convenient foundation for charismatic leaders to whip up into outright hatred? How can we argue against this minority Muslim view of Islam's continued humiliation and manipulation by the West? It is difficult when such perceptions are based on kernels of truth. It is even more difficult when the source of this mind-set finds its roots in religious irrationality.[20]

Historians, theologians, sociologists, and anthropologists confirm that this irrational Islamic hatred of the West cannot be easily exorcized. It was born during the Roman occupation and then reborn during the Crusades. It was inflamed after the collapse of the Ottoman Empire and the Balfour Declaration supporting a Jewish homeland in Palestine. It was further intensified after the creation of Israel in 1948 and the partition of India during independence that same year on terms perceived as anti-Muslim, pro-Hindu. Based partially in reality and partially in imagination, this attitude in the Islamic, especially Arab Islamic, world of victimization is so ingrained as to be almost unapproachable diplomatically.[21]

So if fundamentalist Islamic hatred cannot be fully eradicated, can it at least be managed and minimized to avoid further acts of terrorism? Perhaps. America has already laid the groundwork in this regard by avoiding a rash and provocative response immediately after the attacks. Although probably emotionally justified at the time, we did not launch a nuclear missile at Kabul or Kandahar. Our response was deliberate, rational, and sanctioned under international law. This is important if the response is to be viewed as legitimate by the world and especially by the Islamic world (this will be discussed further in chapter 5).

President Bush set the correct tone for allied operations in Afghanistan by stressing that we were not going to war *against* Afghanistan but *in* Afghanistan. Nonetheless, successful completion of this military mission (driving the Taliban from power and pursuing elements of al Qaeda) is only the first step in a long Afghan journey. The ensuing political aftermath is of equal importance as a demonstration of good faith. When the Soviets pulled out of Afghanistan in 1989, America ended its involvement supporting the Mujahadeen and abandoned Afghanistan to its own devices. Subsequently, the country descended into civil war and chaos.[22] We must not abandon them again. To do so would only be confirmation of the minority Islamic view that America and the West are indifferent and selfishly concerned with pursuing their own interests.

America and its allies must communicate to the Islamic world that the West actually does care about its concerns.[23] We must repeatedly point to past actions undertaken to help Muslim countries: successful intervention in Bosnia to defend Muslims against Serbian aggression; NATO bombing of Serbia despite the absence of UN Security Council authorization to protect Muslim civilians in Kosovo; and even unsuccessful humanitarian intervention in Somalia to avert famine. Then we must translate this message into reality on the ground in Kabul.

Under the aegis of the UN, the establishment of order in Afghanistan has proceeded with invisible Western guidance but with visible Western support (financial and logistic). This balance is delicate but must be maintained. As former ambassador Peter Tomsen put it, we must act "through international support for an internal Afghan dialogue leading to an Afghan regime in Kabul chosen through . . . Afghan consensus. . . . Ultimately, the multiple U.S. interests at stake in Afghanistan can only be accomplished when the majority of Afghans believe their leaders in Kabul have been chosen by Afghans and not from abroad."[24]

The most inclusive form of assemblage convened under a UN conference is the traditional Afghan Loya Jirga. This is a grand council with representatives of every Afghan ethnic, tribal, religious, and political group that historically only convenes for important national decisions. The last assembly was called thirty-eight years ago to ratify a constitution, and one has not occurred to select a new ruler since 1747. Indeed, with the sudden departure of the Taliban, with deposed presidents and lurking kings, and with temperaments fraying among Tajiks, Pashtuns, Uzbeks, and others within the country, the resort to a known and accepted form of traditional decision making could prove stabilizing. Indeed, the Loya Jirga selected interim leader Hamid Karzai as its prime minister for the immediate future.[25]

In tandem with this effort, although perhaps not simultaneously, the United States must revive the aggressive education efforts within the wider Muslim world that it used to pursue during the cold war but unwisely discontinued after the fall of the Soviet Union:

> In the 1980's, when Pakistan was considered a Cold War battleground, American cultural centers were a focus of intellectual and social life in Islamabad, Karachi, Lahore, Hyderabad and Peshawar. Each offered well-stocked libraries, discussion groups led by visiting Americans and a stream of cultural programs. In Lahore . . . singers from the Metropolitan Opera created a sensation, and there were long lines for a show of posters of American paintings. Following a series of budget cuts . . . the ideals, history and cultural vibrancy of the United States were taken off display. . . . Now, thousands of young

> people live at fundamentalist academies where they learn nothing but how to chant the Koran and hate the infidel.[26]

As Allan Goodman, head of the Fulbright scholarship program, notes, "the only way we're going to reduce hatred for America is by giving people some perception of our society, some opportunity to see who we really are."[27] Moreover, we must not continue to sit passively while inflammatory stories air on Al-Jezeera television allowing radical Muslims to cast us in the role of the enemy.[28] Our Department of State must respond on that network, *in Arabic.* Domestically, our political leaders know that allowing one's opponent to define one and one's position in an election campaign cedes power to that opponent that is difficult to regain. This is no less true in our country's foreign relations. America must define itself and not leave that task to others.

In principle, just as we in the West see foreign ambassadors fluent in English defending or explaining the positions of their countries on CNN and MSNBC, our own ambassadors must take to the airwaves. However, in practice, this would be an unmitigated disaster. America's embassies around the world are staffed with ambassadors who have little or no experience in either foreign relations or the specific culture within which they find themselves. They too often owe their jobs to political patronage, measured by how much they helped the current president get elected. Ambassadors of the United States should be qualified individuals, drawn largely from the Foreign Service, familiar with the local culture, and politically astute enough to understand the subtleties of foreign relations.

Moreover, we must reopen American cultural centers and resurrect the educational arm of our public diplomacy. At the same time, we must gradually withdraw public displays of support from despotic regimes whose values are counter to our own, lest we be seen as hypocrites preaching the gospel of democratic principles on the one hand while propping up strongmen on the other. Perpetuating such a hypocritical dynamic ended in graphic failure in Iran with the overthrow of our strongman, the Shah, in 1979. Part of the problem is getting the message through to the masses, perhaps bypassing the state-controlled media through Internet and underground radio usage. As the *Economist* notes:

> If America fails to export a much better side of its culture, its model of freedom—including the freedom to be devout in whatever way you choose, so long as nobody else is hurt—that is mainly because most traditionally Muslim states, including pro-American ones, will not take the risk of opening their air-waves and their printing presses to genuinely pluralist debate. In practice, this has often left the way clear for the message of people . . . like Mr. bin Laden. . . . [H]is kind may be sloppy historians and faulty interpreters of their own faith, let alone others. But even now he could win the propaganda war.[29]

In short, America must engage to set the story straight, espousing our values and ideals, but in a nonthreatening, inclusive manner. We can no longer afford to let our Constitution speak for itself to those who bother to pick it up. The United States must make an effort to display it to the world. But we cannot expect that our version of representative democracy will be adopted wholesale upon presentation, considering anything short of that a failure. Islamic society, especially Arabic society, is ill-suited for immediate democracy. So even limited progress, such as that by Bahrain this year to open parliamentary elections to women, must be encouraged and not criticized because no women were ultimately elected.

From the viewpoint of religion, which of course dominates at least Arabic Muslim culture, Islam, in its classical sense, allows for no separation of church and state. Islamic law, or *sharia,* is not secular; rather, it is law that is ordained by God as interpreted by the clergy. Therefore nonclerical Islamic men who propose framing their own laws, what democracy would consider representatives or parliamentarians, are technically apostates. And historically, the Arab states that emerged from the destruction of the Ottoman Empire inherited borders, like much of Africa, that were drawn in London or Paris for administrative convenience rather than to reflect cultural associations or nationhood. Thus, because the people of these artificial countries identify more strongly with their local tribe or clan and with pan-Arab or the wider Islamic fellowship than with the state, strongmen with strong armies provide the glue that holds the system in place.[30]

As former diplomat Charles Hill explains in his essay "Myth and Reality of Arab Terrorism," there is a

> single approach to the political ordering of [Arab] society. In Oman, a sultan; in Yemen, a military "president"; in Saudi Arabia, a king . . . ; in Jordan, a king . . . ; in Egypt, a president and a parliament only nominally connected to the original Western meaning of these institutions. Beneath all these styles a single form is discernible. Power is held by a strongman, surrounded by a praetorian guard. . . . Every regime of the Arab-Islamic world has proved a failure. Not one has proved able to provide its people with realistic hope for a free and prosperous future. The regimes have found no way to respond to their people's frustration other than a combination of internal oppression and propaganda to generate rage against external enemies. Religiously inflamed terrorists take root in such soil. Their threats to the regimes extort facilities and subsidies that increase their strength and influence. The result is a downward spiral of failure, fear and hatred.[31]

Hill concludes that the impact of this disenfranchisement in Arab society has been undergirded by the "deeply rooted conviction that virtually every significant occurrence is caused by some external conspiracy. Every societal shortcoming is attributed to a foreign plot."[32] Anecdotal evidence of this dynamic is not hard to come by. One of the more persistent rumors circulated and believed by many Arabs—including Mohammad Atta's own father, an Egyptian lawyer—holds that the destruction of the WTC was actually not carried out by Muslims but was rather a plot by Mossad (Israeli intelligence), which is supposedly supported by the fact that four thousand Jews did not come to work at the WTC on September.[33]

Both Russia and America supported these corrupt, despotic systems during the cold war when it suited their purposes. So, the question is, Did that system become more intolerable in the 1990s because the stifling repression by corrupt governments in Arab society increased dramatically or because that system no longer suited the purpose of the great powers, whose forty-year geopolitical chess match had ended and who no longer required obedient pawns—which were much easier to deal with in dictatorial form than in democratic form? The latter is more likely, and the Arabs know it, which is why the argument must shift from one of right and wrong governance (which leads to the dead end of hypocrisy as we condemn dictatorial Iraq, Syria, and Libya while supporting equally antidemocratic Kuwait, Egypt, and Saudi Arabia) to one of a better life offered to the man on the street.

> America cannot change the Arab world at a stroke. It will not risk knocking the legs away from longstanding allies such as Egypt and Saudi Arabia. In wars hot and cold, great powers have collected allies where they can, without too much scruple. But the struggle against forces unleashed by Mr. bin Laden is a most unusual war. Because his aim was to lure the West into an internal quarrel about the future of the Muslim world, it is in large part a struggle about values. The West must not impose its values, but needs to say out loud that its own achievements of religious tolerance and liberal democracy are not just luxuries to be consumed at home. They are universal ideals that can, and should, be welcomed by Arabs too.[34]

Indeed, part of this message could entail simply pointing to the millions of Muslims who live peaceful, contented, religiously fulfilling lives in the West that are often simultaneously economically advanced, politically active, and academically secular. From Hamburg to London to Detroit, Michigan, knowledge of Islamic citizens who have adopted the Western model of democratic freedom but who remain devout might work to ameliorate some of the inaccurate hyperbole directed at the “decadent West” by small-minded fundamentalist clerics seeking to control their own little enclaves of a repressed population.[35]

But in order for this message to resonate, the United States and its allies in the West must avoid government actions that unnecessarily stigmatize Muslims who live in the West or seek to visit. Specifically, the DOJ must issue a detailed statement justifying (in a nondefensive manner) its detention of hundreds of, mostly Muslim, individuals for several months without legal representation. This statement should explain the action, discuss the bases for detention (mostly INS and visa violations), recount the outcome of individual actions (release, deportation, continued detention, etc.), and offer something approaching credible regret about the offensive and discriminatory way in which the action was carried out.

Attorney General Ashcroft must also rethink his proposal to fingerprint and photograph anyone from Iran, Iraq, Libya, Sudan, and Syria who enters the United States, regardless of their prior individual activities. By virtue of the fact that they come from those states, they will be treated as security threats. Beginning in the fall of 2002, this applies to anyone from those countries who holds a nonimmigrant visa over the age of fourteen. And for those who remain in the United States longer than thirty days, they must register with the INS and provide proof of employment, school enrollment, or information on their residence. Moreover, if they fail to register each year, they will be fined, jailed, or deported.[36] This ruling affects about 100,000 visitors annually.

The official justification for creation of this state list is that these are five countries "where terrorists are known to operate."[37] While all of these Muslim states have undeniable terrorist connections, so too do Egypt and Saudi Arabia, which furnished fifteen of the nineteen September 11 hijackers. Yet even though these two countries are more directly linked to the attack on the United States than are the five listed states, they are not included. Presumably, this is due to their current friendly relations with our government.

If Ashcroft's reasoning were in fact valid, then any five countries "where terrorists are known to operate" would qualify for the initial spots on his list—Spain, Russia, Ireland, Colombia, and France (none of which are majority Islamic). However, he selected only Islamic states for his list. What message does this send to the Muslim world? It only reinforces the incorrectly perceived anti-Islamic sentiment by the West. These are exactly the type of wrong-headed government actions that must be tempered to help alter such perceptions. The relatively low benefits gained from such pronouncements pale in the balance against the damage they do to our image in the eyes of average Muslims around the world.

We must remember that the real enemy is hatred, and hatred is not defeated on the battlefield. It is conquered in the hearts and minds of the people who harbor it. On September 11, the hearts of most of the world, including the Islamic world, were with us. Now the task is capturing the minds as well.[38] Today's active, reinvigorated education together with multiple tangible demonstrations of empathy in place of yesterday's sentiment of indifference and pervasive arrogance are essential components of attacking the real enemy. Equally essential is treating the Muslim population at home with due respect. That takes a different kind of mind-set on our part and a more advanced strategy.

There appears to be a recognition of this on the part of the administration. A month after the attacks, President Bush remarked, "How do I respond when I see that in some Islamic countries there is a vitriolic hatred of America? I'll tell you how I respond: I'm amazed. I'm amazed that there is such misunderstanding of what our country is about. We've got to do a better job of making our case."[39] Let's hope that we do. As the respected internationalist cold warrior J. William Fulbright once said, "In the long course of history, having people who understand your thought is much greater security than another submarine."[40]

The Problem of the Suicide Bomber

Obviously, the irrationally disturbed mind cannot be easily reached even with the most aggressive and persistent educational efforts, which we in the West have yet to adequately mount. These are the candidates who are ripe for conversion into suicide bombers. They are perhaps the most devious of delivery devices and the most difficult to stop. Short of building a fence around the intended target, as Israel is now doing around the city of Jerusalem, those bent on destroying themselves along with their prey will use any resource and all their human capacity to achieve their result.

Martyrdom is a tricky business, both for the would-be martyr and the leader who recruits, indoctrinates, trains, and releases him or her. However, the idea of self-sacrifice is a powerful one with long historical antecedents that can be used in the indoctrination effort. The Old Testament, considered holy text in the Jewish, Christian, and Islamic faiths, recounts the compelling story of Samson asking God for revenge against the Philistines and placing himself between two giant pillars supporting a building that he forces apart, burying himself and his intended victims in the ruins:

> And Samson took hold of the two middle pillars upon which the house stood, and on which it was borne up, of the one with his right hand, and of the other with his left. And Samson said, "Let me die with the Philistines." And bowed himself with all his might; and the house fell upon the lords, and upon all the people that were therein. *So the dead which he slew at his death were more than they which he slew in his life.*[41]

The example in that biblical story could not be clearer. By destroying oneself in a heroic way, one's cause may be furthered beyond what one is capable of accomplishing as an individual while alive. This principle is a key element in the strategy of suicide terrorism. Although perhaps a truism, this teaching nonetheless resonates with the right personalities whose hatred has more value to them than their own lives. Moreover, history shows that governments respond to such tactics.

In 1983 a series of suicide car bombings was unleashed by Syrian-backed fundamentalist Shi'ites in Beirut, Lebanon. On April 18 the U.S. Embassy was attacked, wounding 120 and killing 63; on October 23 the U.S. Marine headquarters was hit, killing 241; on that same day the French paratrooper headquarters was attacked, wounding 15 and killing 58. Shortly thereafter French and American forces were withdrawn from Lebanon[42] and the area was left to descend into a decade of chaos and religious internecine warfare occasionally interrupted by overlapping periods of Israeli occupation and Syrian military dominance.

Given such salient religious and historic examples, what base factors come together to create a suicide terrorist? Dr. Ariel Merari, a psychologist and the director of the Project on Terrorism at Tel Aviv University's Jaffe Center for Strategic Studies, has identified four constituent elements: cultural factors, indoctrination, situational factors, and personality traits.[43] When these elements are present and combined correctly, the suicidal mind-set can be exploited for any purpose.

The first element, cultural factors, includes religious motivators. As Merari notes, "All monotheistic religions promise life after death. Hypothetically, they may thus encourage suicidal behavior, especially if the suicidal act is carried out for a righteous cause."[44] And although suicide is formally forbidden in the Jewish, Christian, and Islamic faiths, a clever leader can twist religious teachings to allow that which is forbidden. In Islam, a believer who is killed by the enemy in jihad (holy war) is guaranteed a place in paradise—clearly a tempting alternative to life in the hellish refugee camps of the West Bank, for example. But there is no paradisal place for suicides.

Knowing this, an educated leader may capitalize on the dual hatred nursed in the bosom of the downtrodden together with the potential suicide's lack of doctrinal religious teaching to convince him or her to attain a place in paradise (and also for their family) by joining the falsely named jihad against the West. Thus, martyrdom can be packaged and sold as a one-way ticket to everlasting happiness in the afterlife. In this way, the cultural factors lay the foundation for suicide terrorism to manifest itself.[45]

The second element, the indoctrination itself, occurs on two levels. The first is an educational process whereby the person is "convinced of the importance of the cause and of the means necessary for its implementation."[46] Parents, teachers, writers, and others are participatory agents of influence. The second level is the brief, mission-oriented persuasion task, usually performed by a charismatic political, military, or religious leader, shortly before the attack is to be carried out. The person conducting the indoctrination of the would-be suicide terrorist strengthens already existing convictions laid by the cultural factors and the influence wielders during the education process but adds the element of personal commitment to the cause.

The third element, situational factors, includes the conditions and circumstances surrounding the commission of the attack. If the opportunity (geography, proximity, timing, target awareness, etc.) does not exist, then the situational factors are not contributory in a significant way. But situational factors also include those surrounding the suicide terrorist, such as the possibility of group suicide and the effect of an audience.[47] Group suicide tends to strengthen the resolve, through peer pressure and other mechanisms, to carry the task through to completion. Moreover, the effect of an audience is practically guaranteed in the age of instantaneous electronic media coverage.

Another element that could perhaps be included in situational factors is the prospect of tangible benefit. One of the more interesting components to arise during the Palestinians' second *intifada* against Israeli occupation has been the financial reward bestowed upon the families of successful suicide bombers. Saddam Hussein's Ba'ath Party regime in Baghdad, maybe recalling the unmitigated support it received from Palestinians during the Gulf War, sent cash to family members of dead terrorists. Each family that suffered the loss of a son or daughter in a suicide mission against Israel received twenty-five thousand dollars. In the world of the refugee camp, this dynamic could provide a twisted motivation in itself.[48]

The fourth element, personality traits, is an amalgam of the internal psychologic condition of the potential suicide and the effects of the environment upon him or her. Consequently, it is exceedingly difficult to construct a dependable profile of personality traits that is uniform for potential suicide terrorists. This is made more complicated by the fact that successful ones are consumed in their own attacks, and their personal histories are often not available.

Nonetheless, with respect to the first three of Merari's constituent elements, al Qaeda's success in producing such devastating weapons as suicide bombers in the first WTC attack, the Khobar Towers bombing, the USS *Cole* attack, the bombing of the American embassies in Africa, and then the September 11 attacks inside the continental United States is self-evident. That organization's mastery at exploiting the constituent elements cannot be denied. The cultural factors existed for the indoctrination to take place on both levels. Osama bin Laden provided the charismatic leadership for the second level of indoctrination. Group suicide and the access to a global audience stimulated the nongeographic situational factors, and mobility of the suicide terrorists mitigated the geographic ones.

What can we do to defend against that which cannot be stopped by concrete barriers or intercepted by law enforcement or destroyed by military action? What can we do to defend against those people who are bent on destroying themselves in the process of destroying their perceived adversaries? We must reach out and alter that perception of America as the enemy. Only by taking ourselves out of the role of adversary can we protect ourselves, our interests, and our way of life from suicide bombers.

Thus, we must aggressively proceed on the path laid out in the preceding section to educate the Muslim world about our American values and our support of Islam. Only by defining ourselves and what we stand for can we undermine the power of charismatic Islamic leaders to define us in a distorted manner. In this way, the cultural factors will dissipate over time. Once that foundation evaporates, the first level of indoctrination (through influence-wielding parents, teachers, and writers) becomes more difficult and may dissipate as well, thereby making the job of the charismatic leader in the second level of indoctrination all the more difficult and unsuccessful.

Biological, Chemical, and Nuclear Threats

WMD conjure up scenarios and destructive forms that not only capture the literary imaginations of authors such as Tom Clancy (*Sum of all Fears*) and Stephen King (*The Stand*) but provide many sleepless nights for those in government charged with guarding against their use. Biological, chemical, and nuclear weapons are the WMD most often cited as areas of concern should they fall into the hands of anti-American terrorists.

Historically, such weapons have a long, but limited track record. Biological weapons have been around since the Middle Ages, when commanders laying siege to cities would catapult dead bodies over city walls to spread Black Plague and other forms of pestilence.[49] Chemical weapons were employed by artillery and used in World War I on both the Eastern and Western fronts by the Germans and later in response by the Allies. The nuclear device has been used twice, both times by the United States against Japan during World War II.

Employment of such weapons by states against other states in the latter half of the twentieth century was rare, due largely to the deterrent effect of like retaliation coupled with treaties outlawing their use. Consequently, the emerging threat today is not from other states so much as from terrorist organizations who are immune from deterrence and do not belong to the treaties designed to control WMD. A report by the National Research Council released in the summer of 2002 found that the United States was ill-prepared to deal with a terrorist WMD attack and lacked a "coherent overall strategy."[50] The government is now working to develop one.

Harvard University's Jessica Stern, Senior Fellow at the Belfer Center for Science and International Affairs, has studied terrorist groups in their quest to acquire WMD. She notes that "[c]andidates for employing these weapons are found at the intersection of three subsets: terrorists who want to use the weapons despite formidable political costs, terrorists who are able to acquire or produce them, and terrorists who have the ability to deliver or disseminate them covertly. . . . [T]he area created by the intersection of these sets is small but growing."[51]

At least in the case of Stern's first criterion, religious fanaticism may provide such motivation. The Library of Congress's report to the National Intelligence Council—entitled "The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?"—found that for the most fundamentalist of groups

> [t]heir outlook is one that divides the world simplistically into "them" and "us." . . . The religiously motivated terrorists are more dangerous than the politically motivated terrorists because they are the ones most likely to develop and use weapons of mass destruction in pursuit of their messianic or apocalyptic visions. The level of intelligence of a terrorist group's leaders may determine the longevity of the group. . . . [Osama bin Laden is] the prototype of a new breed of terrorist—the private entrepreneur who puts modern enterprise at the service of a global terrorist network.[52]

In the case of the second criterion, where can such highly determined groups access the WMD in a form that can be easily converted to later use in a terrorist attack? While isolated incidences outside of Eurasia occur, such as the South African biological weapons scientists who offered their expertise to Libya,[53] the main fear rests with the former Soviet Union. When the USSR collapsed in 1991, its massive arsenal of biological, chemical, and nuclear weapons and facilities was inherited by fifteen suddenly struggling independent states that were not only new custodians of WMD but also in dire economic straits. Many of them remain so.

Moreover, the chaotic new legal and political environment in these fledgling democracies (Russia included) remains rampant with corruption and heavily influenced by organized crime, whose networks have provided willing purchasers of WMD material and scientific expertise backed with much needed hard currency.[54] According to Stern, the resulting black market is now offering these items along with their delivery technology. But the danger remains. For example, although "law enforcement authorities have seized hundreds of caches of stolen nuclear materials,"[55] it is impossible to know for certain how many transactions were culminated.

As for the third criterion, covert delivery, small or isolated organizations may find this hurdle insurmountable. However, groups with large, perhaps clandestine followings, such as Japan's Aum Shinrikyo, or groups with widely dispersed networks operating in individual cells with separate destructive capacities, such as bin Laden's al Qaeda, could clear such a hurdle. The possible delivery scenarios are what policymakers have some control over; consequently, the troubleshooting, border and security systems testing, threat analysis, and debates about resource allocation tend to focus on this area. The result is an unsettlingly long catalog of hypothetical doomsday scenarios about which little can be done, but preventative measures must nonetheless take place.[56]

Biological Weapons

The first challenge for governments developing a defense to biological weapons is facing the mental hurdle of segregating that defense from the tendency to lump it together with a coordinated response to other WMD such as chemical and nuclear devices. As Christopher Chyba, codirector of Stanford's Center for International Security and Cooperation, points out, biological, chemical, and nuclear weapons

> [d]iffer greatly in their ease of production, in the challenges they pose for deterrence, and in the effectiveness of defensive measures against them. The post-September 11th focus on WMD and whether they are in the hands of enemy states or groups risks overlooking these complexities. Put simply, biological weapons differ from nuclear or chemical weapons, and any biological security strategy should begin by paying attention to these differences.[57]

Indeed, the unique character of bioweapons is self-evident: they can be secretly introduced to a population through an unknowing carrier (or a knowing one if he or she is a suicide terrorist) without warning; they have the ability to self-perpetuate—widening the circle of destruction exponentially upon introduction; and in many instances there is no known vaccination, treatment, or cure. Moreover, the terror factor, derived from the panic that inevitably ensues from a biological attack, can be an ancillary form of injury as populations scramble to escape the effects of the bioagent. This factor could claim lives too, as accidents occur, hospitals are overrun, evacuations or quarantines spin out of control, or troops are forced to fire on civilians.

Another unique characteristic of biologic weapons that could draw religiously fanatical terrorist organizations to seek them is their metaphoric use as divine retribution. In the Book of Exodus, the fifth plague used by God to punish Pharoah is believed to be murrain—from the anthrax family. And in the Book of Samuel, God unleashes a pestilence on the Philistines that medical historians correlate to bubonic plague. There are other examples, but it is the symbolism and religious connotation of employing a living organism to destroy other living organisms that sets bioweapons apart from chemical or nuclear agents.[58]

These biologic killers come in mainly three forms: bacteria, viruses, and toxins. Bacteria are single-celled living organisms. They are tiny (measured only in micrometers) and range in shape from the spherical cocci to the long, rod-shaped bacilli. The single cell contains DNA, cytoplasm, and the membrane. Some bacteria can transform themselves into spores. If this happens, they lie dormant, like plant seeds, until conditions are right to germinate. Bacteria cause disease in humans by directly invading the tissue, producing toxins, or both. Examples of deadly bacteria that can be utilized for bioterror purposes include anthrax, cholera, and plague, with mortality rates upon contraction of almost 100 percent, 50–80 percent, and 50–100 percent (depending on whether bubonic or pneumonic plague is used), respectively.[59]

Viruses are even smaller than bacteria. They are composed of DNA or RNA and require living cells in order to replicate. They are not self-contained and cannot metabolize on their own. The host cells they need to live and multiply can be human, plant, animal, or bacteriological—but each type of virus requires a specific type of host cell. Normally, this parasitic relationship kills the host cell. The most dangerous viruses include smallpox; a wide variety of hemorrhagic fevers ranging from the most lethal Ebola, Marburg, and Crimean-Congo strains to the less lethal Q fever and yellow fever; and the generally nonlethal Venezuelan Equine Encephalitis.[60]

Toxins are any naturally occurring poisonous substances. Their origin could be animal, plant, or microbe. They are typically not infectious and therefore do not have the potential for a ripple effect that bacterial and virological agents have. Delivery can enhance or constrain the toxin's effect. Some toxins are more toxic when sprayed by aerosol while others can only be delivered orally or via blood-to-blood contamination. The toxins most commonly considered dangerous for bioterror purposes include botulinum, against which humans have no natural defense and which can be converted to powder, aerosolized, and sprayed; ricin, derived from the widely available castor plant and against which antibiotics cannot be used due to the rapidity with which it causes respiratory failure (36–72 hours) when inhaled or vascular collapse if ingested; and the much less lethal *Staphylococcus aureus* toxins, most commonly associated with food poisoning.[61]

Of the three, the United States has the most recent experience with anthrax, which was unleashed domestically through the U.S. mail system after the September 11 attacks by an as yet unknown assailant. When inhaled, spores from this bacterial agent can penetrate deep into the lungs. While the spores are vulnerable to treatment by ciprofloxacin (Cipro), penicillin, and tetracycline, getting the treatment soon enough is problematic.[62] The attacks came in the form of a fine white powder in letters sent to Democratic members of Congress and elsewhere. Experts estimate that the original letters contained one trillion spores.[63]

But four of the five deaths that resulted from the mailed letters were not direct recipients. Rather, they were postal workers and unfortunate individuals who received one of the five thousand letters that were cross-contaminated during the postal routing and handling process.[64] The postal service has used money earmarked by Congress to counter such powdery anthrax attacks in the future. Specifically, they are installing PCR systems at 292 sorting facilities that collect air samples sucked from the mail and test for eight different biohazards (anthrax plus seven that will not be disclosed) and retrofitting their high-speed sorters with vacuums that feed air out of the system and into filters.[65] Whether such measures prove sufficient remains to be seen. Shortly after the September 11 terrorist attacks, the United States and Uzbekistan signed an agreement to clean up an island in the rapidly disappearing Aral Sea, where the Soviet government had dumped tons of weaponized anthrax spores from its illegal biological warfare program in 1988.[66]

The only other time anthrax claimed a larger number of lives in weaponized form in an industrialized nation was when a Soviet military experiment went dangerously awry in 1979 in Sverdlovsk, claiming sixty-four lives according to Soviet sources or thousands according to U.S. intelligence.[67] Anthrax and botulism were used alternately from 1990 to 1995 by the Japanese religious cult Aum Shinrikyo to attack subway systems, the Diet, the Imperial Palace, and the naval headquarters of the U.S. Seventh Fleet in Yokosuka in mist form. However, due to a combination of ineptitude, repentant followers, and insufficiency of the biological agents' virulence, no one was killed; indeed, neither the Japanese nor U.S. governments became aware of the attacks until years later, after the cult had switched to chemical attacks (sarin gas), which proved much more successful.[68]

Nevertheless, the importance of the attempt by the Japanese terrorist group remains significant because it points to the fact that states and their militaries are no longer the sole actors in biowarfare. This, in turn, reinforces the importance of government measures to limit access to these contagions. William Patrick, a former germ warfare expert for the U.S. government, considers limited access the key to protection. He notes that because a specific type of microbe could come in hundreds of subvarieties, but only one strain might pose lethal risks to humans, for bioterrorists "getting the most infectious and virulent culture for the seed stock is the greatest hurdle."[69]

But small organizations, not typically regarded as terrorist, can convince themselves to use the less virulent varieties of germ in order to further their political ends. A nonlethal toxin attack was mounted by followers of the Bagwan Shree Rajneesh in 1984 by sprinkling salmonella typhimurium onto restaurant salad bars in Oregon in an attempt to sway an election. More than 750 people fell ill as a result.[70] Thus, apocalyptic visions of divine retribution can at times give way to achieving more mundane objectives as a motive for use of bioweapons by a fringe group.

Beyond bacteria and toxins, the virus smallpox is emerging as a deadly alternative agent. Eradicated by the World Health Organization as a naturally occurring disease in 1980 and confined to two frozen vials (one in the United States, the other in the USSR), it is apparent that Iraq and North Korea now also have the virus and that China, Libya, South Africa, Israel, and Pakistan are believed to possess it as well. Consequently, the containment policy did not work. During the twentieth century alone, smallpox killed more than 300 million people—more than all the wars of that period combined.[71]

The symptoms of smallpox are unmistakable. Ten days after infection, headache, backache, vomiting, and fever manifest themselves. Then the fever wanes, and the individual begins to feel better. Consequently, one might mistakenly believe that it is the flu. Shortly thereafter, the first red spots appear evenly spaced on the face and extremities. This rash spreads as the spots turn to lumps and fill with fluid that seeps from capillaries, making them hard, like BBs embedded under the skin. Sheets of skin begin to separate and slough off as the disease quickly progresses, which can lead to death within sixteen days from organ failure, pneumonia, or overreaction by the immune system. There is no treatment, only the possibility of vaccination prior to infection. The mortality rate is around 50 percent.[72]

Computer modeling, hypothesizing a not unreasonable single bioterrorism outbreak of one hundred smallpox cases in a typical American city, predicts that the resulting disease "would become a worldwide conflagration in as little as a year" unless an aggressive, large-scale immunization campaign were undertaken to stop it—which is not currently possible. As of 2001, there were only 60 million doses of smallpox vaccine in the world, of which the United States had 8 million. Containment of the outbreak hypothesized in the computer scenario would require 30 to 40 million doses.[73] In response, the Department of Health and Human Services began purchasing enough vaccines for every American, the military innoculated 480,000 personnel, and 38,000 emergency health workers were vaccinated by 2003.[74]

Another viral superbug with exponential ripple-effect capability that government officials worry about is Ebola, strains of which do not even have vaccinations. Graphically recounted in Richard Preston's reality-based novel *The Hot Zone* in 1994, Ebola Zaire and Marburg strains emerged from Africa and through Europe to the United States undetected, living in monkeys kept at a laboratory in Reston, Virginia. The virus jumped from the animals to humans, and, of course, chaos and cycles of human death ensued.[75] Ebola does have that transmutational capacity, as well as the ability to become airborne, which makes it so deadly and unpredictable.

Ten days after infection of Ebola, the flu-like symptoms common to most viruses emerge: fever, vomiting, and achiness. However, the second phase moves more quickly and gruesomely. The virus attacks all organs and tissues except bone and muscle in the body, most of which is progressively turned into "a digested slime of virus particles," as the BBC's Tom Mangold and Jeff Goldberg describe in their documentary book *Plague Wars:*

> As the virus storms through the body making copies of itself, small blood clots appear in the bloodstream, the blood thickens and slows, and the clots begin to stick to the walls of the blood vessels. Eventually, the skin develops red spots . . . which are haemorrages under the skin. Subsequently, spontaneous tears appear and join up, the skin goes soft and pulpy, and can tear off. Soon every orifice in the body begins to bleed. The skin of the tongue can slough off causing indescribable pain. The heart bleeds into itself, the eyeballs fill with blood. And it gets considerably worse before death.[76]

The horrific scenarios by which such attacks can be carried forth are limited only by the imagination, the stability of the biological agent, and the virulence of the strain. Luckily, the latter two actually function as limits on most forms of attack. Only militaries typically have the scientific expertise, discipline, and foresight to successfully mount such attacks. Few terrorist groups would have the know-how to control stability when the agent is converted to delivery form, as well as the proper use of an effective delivery mechanism coupled with the reliability of the agent and its continued potency.[77]

However, this does not solve the problem of former military members with mercenary streaks joining forces with terrorist organizations seeking their guidance—for a price. Delivery can be aggressive: using crop-dusting airplanes, dispersing it in building ventilation ducts, injecting it clandestinely into drinking water aquifers, depositing it into postal systems, or simply tossing a glass vial onto the tracks of an oncoming subway train, whose trailing air vacuum would send the spores dashing through tunnels and onto platforms.

Delivery can also be subtle. Jose Padilla, an al Qaeda operative instructed to scout out targets for a radiologic "dirty bomb" attack, flew from Pakistan to O'Hare Airport in May 2002, where he was apprehended by waiting law enforcement officials. Federal agents patted themselves on the back for effecting his capture, and Attorney General Ashcroft made a valedictory statement from Moscow in that regard. From the government's perspective, the case was closed upon apprehension, and the job remaining to handle Padilla was for lawyers.

But suppose Padilla had been exposed to delayed-effect virological agents like smallpox or an Ebola strain (knowingly or unknowingly) prior to boarding his plane in Karachi. During the thirty-six hours it takes to get to Chicago, he could have contaminated those around him and those who used the washroom after him through fluid contact and could have contaminated the other four hundred passengers and crew breathing the same recirculated air as he was (if airborne contact transmits, as in the case of Ebola). In that time, the flu-like symptoms would not yet have become apparent. Consequently, upon landing, his capture would not matter much. No one else on the plane had been detained—there was no reason to do so.

By the time Padilla's symptoms appeared, perhaps two days before anyone else who was on that plane, those four hundred souls would have driven into their Chicago suburbs or boarded other flights for a hundred other destinations within the United States. They could not be tracked using the flight lists before they died and had infected others. The agents making Padilla's arrest would likely themselves be infected, as well as their families and fellow law enforcement officers and their families. Indeed, by the time patients wandered into hospital emergency rooms around the country with red dots covering their faces, in the case of smallpox, or spewing blood from their eyes and ears, in the case of Ebola during what is called a "bleedout," containment would be impossibly difficult (perhaps requiring martial law) and treatment not an option for those already infected.

So what have we done to respond legally to this threat? Domestically, the unauthorized manufacture, trade, sale, or public exposure of such biological agents is illegal under Titles 18, 22, 42, and 50 of the U.S. Code and several executive orders. This web of laws also criminalizes attempts and conspiracy. Moreover, shipment of deadly bioagents has been monitored since 1997; however, no development of a gene library creating a national inventory of these diseases or consolidation of facilities with the most dangerous strains has been undertaken. According to Stanford's Dr. Chyba, had these efforts been in place in the fall of 2001, "the anthrax investigation could have proceeded more quickly."[78]

Internationally, deterrence through the threat of massive retaliation has been the key strategy relied upon to prevent the use of these agents. However, deterrence won't work against a terrorist organization that does not care if it is eradicated (or martyred) or that has dispersed by the time the United States figures out the biological agents' point of origin. The 1972 Biological and Toxin Weapons Convention prohibits production and stockpiling of the agents, and the 1925 Geneva Protocol prohibits their use. However, the Bush administration rejected the compliance and verification protocol to the treaty in July 2001, arguing that it would "jeopardize U.S. [pharmaceutical] companies' proprietary information, did not provide sufficient protection for U.S. biodefense programs, and would not improve verification capabilities."[79]

Nonproliferation is a related but separate concern from noncompliance. The goal of nonproliferation is less easily reached in the context of deadly biological agents than it is in the context of nuclear weapons. Scientists can come by potentially lethal germs or toxins in the course of otherwise legitimate, perhaps university-backed or federally funded research. Naturally occurring disease outbreaks are another source of these organisms—witness the continual recurrence of the Ames strain of anthrax in eastern Texas.[80]

Artificial construction of such diseases is yet another possibility. In the summer of 2002, the *New York Times* reported the success of scientists at the University of Buffalo–Stony Brook in their quest during a Pentagon-funded study to create a synthetic version of polio from chemicals and publicly available information:

> The scientists constructed the virus using its genome sequence, which is available on the Internet, as their blueprint, and genetic material from one of the many mail-order companies that sell made-to-order DNA. Dr. Eckard Wimmer, professor of molecular genetics and microbiology at Stony Brook and leader of the project, said they made the virus to send a warning that terrorists might be able to make biological weapons even when they could not obtain a natural virus. "You no longer need the real thing in order to make the virus and propagate it." The work immediately set off a debate over whether the same technique might be applied to other viruses. The genetic codes for many dangerous pathogens, including smallpox and ebola, are freely accessible on the Web. And the team relied on technology that is generally available in molecular biology labs around the world.[81]

It is also unclear whether bioweapons technology has remained contained by the superpowers since the end of the cold war. Indeed, the Soviets flagrantly violated the terms of the 1972 treaty for two decades prior to their country's collapse—a fact we in America did not become aware of until 1989. The man who ran the Russian bioweapons program as deputy chief of Biopreparat from 1988 to 1992, Ken Alibek, defected to the United States in 1992 and is now a citizen. He discloses in his book *Biohazard* the extent to which Russian efforts to capitalize on their scientific expertise in this area continue:

> In July 1995, Russia opened negotiations with Iraq for the sale of large industrial fermentation vessels and related equipment. The model was one we had used to develop and manufacture bacterial biological weapons. Like Cuba, the Iraqis maintained the vessels were intended to grow single-cell protein for cattle feed. What made the deal particularly suspicious was an additional request for exhaust filtration equipment capable of achieving 99.99 percent air purity—a level we used only in our weapons labs.
>
> Negotiations were called off by the time reports of the deal surfaced in the Western press, but a United Nations employee told me Iraq obtained the equipment it needed elsewhere.

> United Nations Special Committee Inspection Teams, established after the Gulf War to monitor the dismantling of Iraq's chemical and biological weapons programs, had not been able to find this equipment by the time they were ejected from Iraq in late 1998. Many similar deals have gone undetected. . . . In 1997 Russia was reported to be negotiating a lucrative deal with Iran for the sale of cultivation equipment including fermenters, reactors, and air purifying machinery. The equipment was similar to that which was offered to Iraq.[82]

Given the failure of states to comply with the treaty prohibitions, the increased realization that bioagents are widely available, and the first biological attack on the United States last fall, Congress passed legislation, signed by the president in June 2002, to provide $4.3 billion for drugs, vaccines, training, and other initiatives to prepare for further biological attacks. This includes tightening security at water plants, improving food inspections, and increasing stockpiles of smallpox and other vaccines. Another $1.6 billion is earmarked for distribution to states and localities—recognizing the fact that such attacks must be initially identified and tackled by first responders at the local level.[83]

Localities will spend the money on new protective gear, mobile laboratories, pathogen testing equipment, traffic control (new lights and video technology), and hazmat equipment for fire departments. After decades of neglect, these disbursements amount to the first step on the part of the federal government to build a robust biodefense system centered on the key elements of quick response, containment, treatment, and panic control. But it is expected to take years for the system to ramp up to where it needs to be to prove effective.[84]

Chemical Weapons

Chemical weapons have been used more extensively than biological weapons. Although tried on the Russians six months earlier, the first large-scale chemical attack came during World War I when the Germans released a five-mile-wide cloud of chlorine gas against the French in Belgium on April 22, 1915. There were fifteen thousand casualties and five thousand deaths. By 1918 both sides employed the technology and one in four artillery shells fired contained a gas component. Adolph Hitler, a corporal in the German army, was temporarily blinded by a British gas attack in Flanders—which many believe led to his decision not to employ it as a weapon in military operations during World War II. In fact, no major power has employed the use of chemical weapons in combat since that time.[85] This, of course, does not rule out the possibility of their future use, either by corrupt regimes of rogue states or by terrorist organizations.

Chemical weapons come in three types of agents based on the area of the body they affect: choking, blistering, and nerve agents. Choking agents include chlorine and phosgene gases. They attack the respiratory tract, destroying pulmonary capacity in about four hours, leading to death. Blistering agents include the family of mustard gases and lewisite. These agents cause blisters on the skin and destroy substances within living cells—attacking the eyes, mucous membranes, internal organs, and respiratory tracts. They are slower acting (taking effect twelve to twenty-four hours after exposure) and less deadly, although death can result from lung injury. Nerve agents include sarin, tabun, somoan, and VX. They disable enzymes that transmit nerve impulses, the incapacitating effects of which are felt within ten minutes. Death invariably occurs within fifteen minutes unless VX is used, which has a longer mortality (and suffering) time line of four to forty-two hours.[86]

These agents can be dispersed as liquids, vapors, gases, and aerosols; however, the effectiveness of the attack can be compromised by the method of dispersal, which is closely linked to the chemical used. In the case of munitions, the explosive device must be constructed such that it does not destroy the chemical intended for deployment. In the case of sprayers or liquid dispersal, the delivery media must be carefully measured such that it does not dilute the chemical to the point of impotence. Scientific and engineering accuracy are the keys to success.

Chemical weapons were used by both sides in the Iran-Iraq War from 1980 to 1988, and Saddam Hussein used them to devastating effect against his own countrymen to put down the 1987–88 Kurdish rebellion in the north. However, Iraq did not employ them against American-led coalition forces or against Israeli SCUD rocket targets during the Gulf War in 1991, largely in response to a specific threat by the United States that such an attack would be met with an overwhelming nuclear response. Prior to the recent regime change in Iraq, Iraq and Iran continued to have an antagonistic relationship; thus, they continued to manufacture and stockpile chemical weapons despite negative international pressure (and UN Security Council prohibition in the case of Iraq) due to strategic concerns vis-à-vis each other.[87]

Sarin gas was the weapon used by the apocalyptic Aum Shinrikyo religious/terrorist group in its 1995 attack on the subway system in Tokyo. The cult's followers carried frozen packets of sarin onto the trains during the morning rush hour, poked holes into the packets with sharpened umbrella tips, and then exited the subway as the packets began to thaw and poison the commuters. Over five thousand people were injured by the nerve agent, and eleven people who were in closest proximity to the exposure died. The Tokyo attack followed an earlier sarin attack that year on the Japanese city of Matsumoto, about one hundred miles north, where seven people were killed and six hundred sickened.[88]

This was the culmination of the group's ineffective attempts during the prior five years to use biological weapons. Technical difficulties controlling the strain and the dissemination method led to repeated failures. Aum Shinrikyo also tried but failed to obtain usable nuclear weapons. Consequently, chemical weapons were the third and last choice of WMD that the group finally used with limited success. Had the group been able to use a purer form of sarin and a more effective, focused delivery device, the 1995 attacks would have been far worse. Consequently, while the failures of the group are instructive, its "success" supports the theory that such organizations may continue to acquire WMD and that WMD usage is no longer limited to governments and militaries.[89]

So how is this material controlled so it will not fall into the hands of such organizations? The Chemical Weapons Convention (CWC), formally adhered to by 143 nations but not always in practice, prohibits the production, testing, and use of chemical weapons and is designed to eliminate already existing stockpiles—mostly through incineration. The United States joined the CWC with its ratification in 1997. Through inspections and supervision, the Organization for the Prohibition of Chemical Weapons (OPCW) deploys more than two hundred experts to accomplish its task.[90]

Battlefield evidence gathered by American forces in Afghanistan, however, indicates that al Qaeda had some chemical weapon capability and was working on perfecting and expanding that capability.[91] This raises the question of where such organizations can obtain this material. If the CWC is working, then terrorist groups should not be able to acquire it. Actually, the CWC is not working all that well.

The OPCW has been underfunded since its inception, forcing them to cut back from 98 to only 42 military inspections and from 132 to only 61 industry inspections in 2001. Key countries with known or suspected stockpiles and delivery capability, but questionable security, either have not joined the CWC, as in the case of Egypt, Syria, Iraq, North Korea, and Lebanon, or have signed but not ratified the treaty, as in the case of Israel and Libya.[92] But even for those that sign or ratify the treaty, compliance is often not a high priority—as is the case with Russia.

Russia solemnly pledged in the spring of 2001 to begin destroying forty thousand tons of lethal chemical weapons from its massive stockpile (the largest in the world) at three new destruction plants designed for that purpose. After more than a year of noncompliance and dithering, Russia still had forty thousand tons of chemical weapons on its hands. By the summer of 2002, the Group of Eight industrialized nations agreed to match the $10 billion earmarked earlier by the United States to speed the process along.[93]

But even if terrorists cannot get the chemical materials they need from "leaky" states like Russia or one of the former Soviet republics that inherited abandoned testing, storage, and production facilities and that continue to worry the West, they can take advantage of sitting ducks. By targeting a chemical processing facility close to a population—850,000 dot the American landscape and thousands more are scattered across Canada and Europe—when it happens to be running a particularly lethal and explosively gaseous substance, the terrorists' job is made all the easier.[94]

For example, the 1984 accident at the Union Carbide plant in Bhopal, India, killed seven thousand people when cyanide was leaked into the surrounding community.[95] And that was only an accident. Clearly, security must become a top priority at private industrial facilities. Otherwise, terrorists seeking to employ chemical agents in their destructive plans may be able to avail themselves of both the lethal substance and the delivery device simultaneously—without spending vast sums of money on scientific or engineering know-how, chemical acquisition, storage, or transportation.

Nuclear Weapons

At an undisclosed location near Kabul, on a cold November night with the sound of antiaircraft guns booming in the distance, Osama bin Laden confided to Hamid Mir, editor of the Urdu newspaper *Ausaf,* during an interview that "we have chemical and nuclear weapons as a deterrent and if America used them against us, we reserve the right to use them." The White House responded that they took this threat seriously.[96] To date, nuclear weapons have not been utilized by the United States or al Qaeda. Nonetheless, shortly after September 11, the United States rerouted low-altitude planes around nuclear facilities and the National Guard was activated to protect them. European countries also secured their nuclear arsenals and power stations, some such as France and Hungary positioning surface-to-air missiles near them.[97] So far all is quiet.

Indeed, nuclear weapons have not been successfully employed by a state or substate group since the United States dropped two atomic bombs on Japan to end the Pacific conflict and World War II. Not even the recent dust-up between India and Pakistan that took those rival nations to the nuclear brink over the disputed province of Kashmir resulted in the use of these weapons. It is the finality of a nuclear explosion that causes one to pause and think before employing it as a weapon. As technology progressed from atom to hydrogen to plutonium to neutron bombs, the devastative capacity of nuclear weapons increased exponentially. Consequently, their use by rational actors remains a remote possibility, while simultaneously their acquisition remains a priority for security and status reasons.

Most states are rational actors, influenced by such notions. But are terrorists rational actors? It is impossible to answer that question. Thus, states conservatively must assume the worst—that they are not and that if they obtain the technology they will use it. The threat derived from terrorist nuclear capacity is of two types. First is the extremely unlikely, but far more devastating possibility of a terrorist successfully detonating a nuclear weapon. Second is the more likely, but less destructive radiological attack—exploding a conventional bomb laced with radioactive material (known as a dirty bomb) or sabotaging a nuclear facility. In either case, the nuclear avenue of attack was reluctantly admitted by Office of Homeland Security director Tom Ridge to be the most worrisome of all the WMD options.[98]

As for the first type of threat, there are only eight countries known to have nuclear weapons: Russia, America, China, Britain, France, Pakistan, India, and Israel—all of which have supported America's war on terrorism after the September 11 attacks. However, despite assurances to the contrary and the existence of the Nuclear Non-Proliferation Treaty, there is worry that one of the world's twenty-five thousand nuclear warheads could find its way into the wrong hands. And it only takes one. Russia and Pakistan have the poorest records in this regard.

Russia currently maintains the largest nuclear arsenal—fifteen thousand warheads (both strategic and tactical). A recent treaty with the United States commits Russia to reduce its strategic missile-tipped arsenal by about thirty-eight hundred, still leaving it in charge of the largest stockpile of nuclear material. But the caretaker of this heavy responsibility has been described as a country with "sloppy accounting, a disgruntled military, an audacious black market and indigenous terrorists." All of the high-profile arrests in Munich, St. Petersburg, Vienna, and Prague during the early 1990s were of smugglers attempting to escape with Russian nuclear material. But as one official of the International Atomic Energy Agency (IAEA), which tracks these arrests, noted, "Are we seeing half the iceberg or only the tip?" For comparison, drug enforcement officers only consider their police seizures to represent 10–20 percent of what is actually shipped.[99]

Since European controls have tightened, Turkey has emerged as the favorite route for smugglers to get nuclear material out of Russia. In the last eight years, Turkey has intercepted 104 attempts to smuggle mostly uranium, but sometimes plutonium (non–weapons grade), across its frontier. The country is slightly bigger than Texas and has 120 border posts that include crossings to neighboring Iraq and Syria in the south, Bulgaria in the north, and Iran, Georgia, and Armenia in the east. Only two of those posts are outfitted with radioactive detection devices—both donated by the United States.[100] Thus, Russia continues to leak nuclear material; it is just the direction that has changed. According to the Department of Energy, after ten years and millions of dollars in American subsidies, only 41 percent of Russia's weapon-usable nuclear material has been secured.[101]

Pakistan, which built its own nuclear weapons program by using the black market to obtain expertise and material, is the other member of the nuclear club that presents some worry. However, Pakistan stores its nuclear weapons disassembled in different locations; so a smuggler would typically only be able to obtain several parts at a time. Even so, the close relationship between members of the Pakistani military, government, and nuclear research division and elements of the Taliban and al Qaeda give the West reason to worry. Pakistan, however, remains reluctant to accept security assistance from the West, as Russia has done, for fear that India would learn its nuclear secrets. But while the Pakistani option remains a largely unexplored one, the small size of its nuclear program (only twenty-five to forty weapons) means that there is less material available.[102]

Assuming terrorists did manage to secure a nuclear weapon, the technological hurdles they would face to cause a detonation are considerable. American warheads are rigged with multiple permissive action links, which are codes and self-disabling devices meant to keep an unauthorized person from detonating the warhead. Russian weapons are similarly rigged. General Eugene Habiger, formerly in charge of the American strategic weapons unit, explained that a terrorist would have to take the weapon apart to make it work, and the failsafes are so complex that it would be easier to extract the plutonium or enriched uranium from the core and build an entirely new weapon.[103]

This is reassuring in the context of the big strategic weapons, but how about the smaller tactical weapons—nuclear torpedoes, depth charges, mines, and artillery shells? Their antiuse devices are less sophisticated because these weapons are meant to be used on the battlefield—and the older tactical weapons have no such devices. That element, coupled with their smaller size, greater number, and lack of coverage by a formal treaty regime (which means they are not counted or inspected), as opposed to their larger strategic cousins, makes them prime targets for theft. Consequently, we must rely on the inherently unreliable border, surveillance, and facility security.

Beyond ready-made weapons, the second option for a terrorist seeking to employ a nuclear method of attack is radiological dispersion using a dirty bomb—which is actually not a nuclear bomb at all. Rather, it is a conventional bomb made of traditionally widely available explosives (TNT, fertilizer, plastique, etc.) and laced with radioactive material, which is equally abundant. Three types of such elements—cobalt-60, americium, and cesium-137—are commonly used in food processing to kill bacteria, in hospitals for medial gauges and radiotherapy machines, and in items such as smoke detectors and equipment for oil prospecting, in addition to the many academic and industrial research laboratories across the country.[104]

This solves the problem of terrorists having to import their tools of destruction. They can simply find them in the United States. The Nuclear Regulatory Commission (NRC) reported in 2002 that U.S. business, industrial, and medical facilities lost track of almost 1,500 pieces of radioactive equipment since 1996. Of this, about 660, or 44 percent, had been recovered, but the rest remain "missing." Penalties and fines have been issued against some of the institutions, very little of which has been collected. Similarly, a 1995 Department of Energy inventory determined that "tens of thousands" of the agency's radioactive elements could not be accounted for. Many of the items are thought to have ended up in dumps and scrap yards—posing additional contamination risks to workers there.[105]

The actual disaster following detonation of a dirty bomb would flow not from the explosion itself, which would kill hundreds, or from the radiation that ensued, which would contaminate hundreds more, but from the mass panic that would result. A report issued by the Center for Strategic and International Studies (CSIS) for the Metropolitan Washington Council of Governments found that a four-thousand-pound dirty truck bomb detonated on Washington, D.C.'s National Mall in a bus would contaminate about 20 percent of downtown but would present a long-term risk of increased cancer or cataract rates in people exposed only a few blocks around the blast site.[106]

However, the psychological effect on the surrounding population would be catastrophic. The responses elicited by a group from local government and emergency response workers at a workshop indicated that a dangerous spontaneous mass evacuation of the Virginia–D.C.–Maryland metro area could not be contained. The report said that "the presence of radioactivity was an issue that the participants were clearly not prepared to deal with." Unlike their local counterparts, federal authorities have taken some preventative action, deploying radiation sensors around the capital, placing a commando unit on standby, and testing various delivery scenarios using boats on the Potomac River and trucks on Interstate 95.[107]

Poorly guarded nuclear waste at weapons facilities and power plants also poses tempting targets for terrorists to exploit in their search for radiologic material. Moreover, if acquisition, stabilization, transport, and detonation present insurmountable technical or logistical problems for the terrorist group, then it has the same option that the terrorist group seeking to utilize chemical weapons has—bypass those issues by exploiting an already existing nuclear facility located near a population center. The Three Mile Island meltdown of 1979 in Pennsylvania demonstrated the panic scenario that would ensue if a reactor were attacked, regardless of success. And the Chernobyl meltdown in the Ukraine graphically demonstrated the contaminative capacity that poorly contained radiologic material has if such an attack were indeed a success.

Internationally, although the IAEA attempts to coordinate threat assessment and security, it is ultimately up to each country to determine its own security needs. Even transnational shipping could be a target. For example, in July 2002, a ship set sail from the Japanese port of Takahama with 550 pounds of almost weapons-grade plutonium for reprocessing in Britain—an eighteen-thousand-mile voyage. It relied for security on several deck-mounted 30-millimeter guns manned by a crew of thirteen British officers employed by the U.K. Atomic Energy Authority Constabulary and on a second vessel similarly outfitted. There was neither official naval escort, as was common practice in the 1980s, nor radar-controlled defenses to guard them from attack by small aircraft or fast boats.[108] No international legal regime is currently in place to require further security measures.

Domestically, America's 103 nuclear power stations are supervised by the NRC. However, for the most part they are on their own to hire private security. Disturbingly, many nuclear facilities routinely fail security breach scenarios designed by the NRC to weigh in favor of defense. In these mock drills, typically only three assailants are allowed with one person working inside, and any variation from the rules, such as improvising the use of a wheelbarrow to cart off material, while successful, disqualifies the study. Some plants even have a less than 50 percent success rate of withstanding a breach in security by ground agents. This does not take into account the lax security under the Department of Energy at the nation's ten nuclear weapons research facilities or the horrific potential of a plane crashing into such a facility or plant—a scenario for which no drill exists.[109]

To counter the effects of a meltdown resulting from an attack, the NRC has offered free potassium iodide pills to thirty-four states that have populations living within ten miles of nuclear power plants. Thirteen have accepted. The pills are to be distributed at homes, schools, and workplaces because immediate administration is critical; however, people are only supposed to be instructed to take the pills if health authorities predict that radiologic exposure is high enough to destroy their thyroid.[110] But not all of the government responses have been adequate or permanent.

In the spring of 2002, the secretary of energy requested $397.7 million to increase security guarding the nation's nuclear weapons, materials, and radioactive waste—as he put it in his letter, "a critical down payment to the safety and security of our nation and its people." However, the White House's Office of Management and Budget cut that request by 93 percent (only $26.4 million) when the executive's budget was sent to Congress.[111] Moreover, temporary measures implemented in the aftermath of 9/11, such as rerouting flight paths around nuclear facilities and placing police and National Guard units at those sites, are expiring. As the extra measures disappear, none has emerged on the horizon to replace them, despite the suggestion from some experts to federalize nuclear plant security forces.[112] Perhaps the new Department of Homeland Security will provide new measures, but until that happens a critical gap in coverage now exists.

Cyberterrorism: The Twenty-first-Century Threat

In August 1999 the Center for Study of Terrorism and Irregular Warfare issued a detailed report analyzing the threat of cyberterrorism. Based upon its analysis, the center concluded that "the barrier to entry for anything beyond annoying hacks is quite high, and that terrorists generally lack the wherewithal and human capital to mount a meaningful operation." The report effectively dismissed cyberterrorism as a real threat, noting that it was a prospect far into the future, although it could be used as an ancillary tool to other physical attacks. Fast-forward to June 2002. The FBI began examining a suspicious pattern of surveillance emanating from the Middle East and South Asia exploring digital systems used to manage Bay Area utilities and government offices. Upon further investigation, the FBI learned that these activities were part of a much larger reconnaissance effort and eventually traced multiple instances of Internet Web browsers routed through Saudi Arabia, Indonesia, and Pakistan, apparently studying emergency telephone systems, electrical generation and transmission, water storage distribution, nuclear power plants, and gas facilities.[113] Thus, where cyberterrorism is concerned, *the future is now,* and, indeed, some government experts have concluded that "terrorists are at the threshold of using the Internet as a direct instrument of bloodshed."[114]

What Is Cyberterrorism?

According to Professor Dorothy Denning, cyberterrorism is

> the convergence of terrorism and cyberspace . . . [and] is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear.[115]

To illustrate her point, Denning further circumscribes the categories of violence against persons or property necessary to rise to the level of a cyberterrorism attack. For example, terrorists gaining access to and tampering with an air traffic control system resulting in a plane crash would be deemed cyberterrorists, as opposed to those disrupting nonessential services, such as defacing a corporate Web page, which results in little more than a costly nuisance to the company involved.

Ironically, the type of cyberterrorism described by Denning is an emerging threat precisely because the global digital revolution has achieved unparalleled success in bringing the world closer together politically, socially, and economically. High-technology tools and services such as the Internet, e-mail, and e-commerce enable people to communicate and transact business across global boundaries, often with the simple click of a button. Thus, while the advent of the technological revolution has been a boon to worldwide social and economic development, it is also very susceptible to manipulation by criminals, who can quickly and effortlessly research and perpetrate harmful deeds across the communications infrastructure. As might be expected, the vulnerabilities inherent in this immensely complex global interconnection of networks have not escaped notice by those bent on exploiting technology for their own terroristic objectives. Indeed, "[t]here is no shortage of terrorist recipes on the Internet . . . [and] step-by-step cookbooks for . . . cyberterrorists."[116]

Consequently, if technologically open societies such as the United States do not take steps now to address this nontraditional threat, which analysts have termed "information warfare," then they could be confronted with cyberterrorism on the scale of an "electronic Pearl Harbor" in the immediate future.[117] Although the United States has yet to experience cyberterrorism on a widespread basis, there are certainly telltale signs that such destructive behavior could be in the offing. Unfortunately, there are also indications that many private and government entities would be ill-prepared to contend with such an eventuality. Consider the following documented cases of cyberterrorism around the globe:

- In the spring of 1999, during the Kosovo conflict, "hactivists" protesting the NATO bombings deluged NATO's computers with "ping attacks," which effectively occupied their computers with a flood of requests and denied service to others seeking legitimate access to the NATO Web site.
- In February 1998 an Israeli hacker, Ehud Tenebaum (aka "The Analyzer"), in collaboration with two California

youths, launched attacks against Pentagon systems, the NSA, and a nuclear research lab. Their handiwork successfully disrupted troop deployments to the Persian Gulf, leading Deputy Secretary of Defense John Hamre to conclude that the cyberterrorists executed "the most organized and systematic attack on U.S. defense systems ever detected."[118]

- Also in 1998 ethnic Tamil guerillas inundated Sri Lankan embassies with eight thousand e-mail messages a day for two weeks, with statements that read, "We are the Internet Black Tigers and we're doing this to disrupt your communications."
- In March 2000, the Japanese Metropolitan Police Department unwittingly procured a software system from the Aum Shinrikyo cult, which was responsible for releasing the deadly sarin gas in the Tokyo subway five years earlier that killed twelve people and injured six thousand more. The software was used to gather classified tracking information on police vehicles, including unmarked cars.

In the United States, according to various reports, almost every Fortune 500 company has experienced at least one unauthorized digital intrusion, many resulting in the theft of data, with an estimated cost of $10 billion per year to companies and consumers. Unwilling to shatter consumer confidence in technology and concerned about potential liability to shareholders, many companies intentionally forego reporting these intrusions and instead choose to silently enhance their security systems, accepting any financial losses as a cost of doing business in this age of technology. Similarly, on the governmental front, tens of thousands of probing attacks are launched against Pentagon systems every year, and information warfare specialists at the Pentagon estimate that a "properly prepared and well-coordinated attack by fewer than thirty computer virtuosos strategically located around the world, with a budget of less than $10 million, could bring the United States to its knees."[119] In fact, there is already some evidence that technology infrastructure attacks apparently originating in countries hostile to United States have been perpetrated against critical government hardware and software systems.

In 1996 the Defense Science Board, in a document entitled "Report of the Defense Science Board Task Force on Information Warfare," identified one of the key impediments to fighting the battle against cyberterrorism:

> Within this rapidly changing, globally interconnected environment of telecomputing activities it is not possible for a person to identify positively who is interconnected with him or her or know the exact path a message and voice traffic takes as it transits the telecommunications "cloud." It is not possible to know . . . how the various software components . . . interact together [or] . . . if the various components installed in computer hardware only do what is asked of them. . . . In sum, we have built our economy and our military on a technology foundation that we do not control and which, at least at the fine detail level, we do not understand.[120]

The task force report also observed that the United States is an information and information systems society, with interconnected and interdependent systems and networks that form the foundation for critical economic, diplomatic, and military functions.

In addition to the exposure occasioned by the interconnection of vital systems, three additional factors exponentially increase the vulnerability of U.S. systems: globalization, which encourages worldwide information exchange and interdependence; standardization, which, although cost-effective, standardizes vulnerabilities across the spectrum; and regulation/deregulation, which often mandates open network architectures, thereby increasing possible points of access to critical infrastructure systems. Taken together, all of these seemingly innocuous features make the United States one of the most vulnerable nations to a variety of cyberattacks, ranging from rogue hackers for hire to state-sponsored attempts designed to gain economic, diplomatic, or military advantages.

According to the Defense Science Board, the overall risk of such an attack upon the U.S. information infrastructure is considerable and best captured in the following equation:

$$\text{Risk} = \frac{\text{Threat} * \text{Vulnerabilities}}{\text{Countermeasures}} * \text{Impact}$$

The threat is very high, as evidenced by persistent probes and attacks against critical governmental systems. The success of many of these attacks indicates that the vulnerabilities are numerous and are a function of the interconnected and interdependent network infrastructure. Although America is lumbering toward designing and implementing solutions to its technology security conundrum, current countermeasures are woefully inadequate to respond to the potentially overwhelming cyberterrorism threat. Consequently, the impact of a targeted attack on America would be catastrophic, prompting the overall conclusion that America is confronting a vast, and potentially deadly, risk that critical infrastructure systems could be devastated and rendered inoperable unless effective countermeasures are initiated and executed posthaste.

What Is Information Warfare?

Even before the digital revolution, information was a choice commodity in the sense that its creation and exchange were essential to building bridges of communication between families, communities, states, and nations. Because the means to convey information in an open society are almost always universally available, they are often taken for granted, and it is generally expected that such capabilities will be reliable and regularly accessible. In other words, whether consciously or not, the United States is a society that depends heavily upon the ability to receive and convey information across the communications infrastructure.

Information warfare takes advantage of this inherent dependency and "is attractive to many because it is cheap in relation to the cost of developing, maintaining, and using advanced military capabilities."[121] Indeed, potential terrorists can utilize the vast and readily available information resources to "suborn an insider, create false information, manipulate information, or launch malicious logic-based weapons against an information system connected to the globally shared telecommunications infrastructure."[122] For example, many Web sites today offer detailed information concerning governmental and corporate structures and systems. Often these data are provided in digital form to enhance the government-citizen and corporate-consumer relationships by maximizing the flow of critical information, while simultaneously lowering the costs of providing such information on an individual basis. But just as this glut of information is readily available to those with benign purposes, it is also easily co-opted by those with criminal intentions. In fact, investigators found that one al Qaeda laptop discovered in Afghanistan had repeatedly visited a French Web site run by the Societé Anonyme, which advertised a two-volume on-line "Sabotage Handbook" complete with tips on planning a digital "hit," computer switch gear, and implementation and antisurveillance methods.

State-of-the-art encryption technology also makes it easier for terrorists to conspire and plan their attacks across international boundaries with little or no detection. For example, Ramzi Yousef, who is currently serving a life sentence for the first WTC bombing, is said to have used his computer to develop and secretly communicate with others concerning a plot to destroy at least a dozen American airlines over the Pacific Ocean. Likewise, it is commonly acknowledged that Osama bin Laden's al Qaeda network frequently uses sophisticated technology devices, such as satellite uplinks and cryptography, to plan and perpetrate their terrorist activities across the globe.

Although information warfare generally connotes using information to one's tactical advantage, the ease of access to information and the means of communication can also facilitate information warfare attacks on the infrastructure itself. Such attacks may arise from within or without the communication network, ranging from physically destroying the system to rendering it useless by disrupting or denying legitimate access. Moreover, depending upon the magnitude, an infrastructure assault may result in the loss of sensitive or critical information or services. In these instances, while the cyberterrorism activities may not directly harm anyone, they might well be a supplemental aspect of a much broader attack. Terrorists might, for example, use information warfare to disrupt or disable a 911 emergency system in conjunction with a traditional bombing assault.

Regarding the tools of the trade necessary for information warfare, cyberterrorists utilize a variety of technology weapons (all readily available on the Internet) to accomplish destructive acts, including Trojan horses, viruses, worms, and denial of service attacks. Such nontraditional weapons and methods of attack are uniquely appealing to the terrorist mentality because individuals and groups can effectively challenge the defensive capabilities of more powerful countries without physically crossing sovereign borders or owning a single traditional warfare weapon. In that sense, information warfare might be considered the "great equalizer."

Like most modern-day terrorist attacks, information warfare designed to further violent agendas is unlikely to be haphazardly planned and carried out. Instead, to maximize harm and increase fear, true cyberterrorism is usually the manifestation of well-organized planning against strategically selected targets. Because the intent is to inflict considerable physical or psychological damage, such attacks are generally leveled against high-profile infrastructure apparatuses. Such detailed planning and implementation, expressly designed to increase the magnitude of harm, is typically referred to as strategic information warfare and is distinguished by the fact that terrorists elect to tactically use information warfare over an extended period of time to accomplish a very specific set of goals. According to a CSIS task force report entitled "Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo," strategic information warfare adds a modern gloss on the historical notion of strategic warfare, which "deduced that it was often more effective to attack an opponent's factories, cities and transportation centers, than to defeat its armies on the battlefield." Moreover, "strategic information warfare offers the ability to target an opponent's information infrastructure directly in order to achieve a decisive victory or competitive edge. . . . Strategic information targets are . . . selected for their ability to cause the systematic collapse of an opponent's capabilities and ability to resist."[123]

For example, one implementation of strategic information warfare might utilize sophisticated technology to surreptitiously evade trade embargoes and sanctions imposed upon disfavored countries. That is, in an effort to skirt the restrictions, a country might develop and implement software to infiltrate banking systems worldwide, skimming money over time from targeted accounts. The purloined funds could then be used to sustain the embargoed government and build its military arsenal, possibly including the acquisition of biological or chemical weapons and technology.[124] In other iterations, terrorist organizations determined to embarrass corporate elitists while simultaneously broadcasting the group's propaganda message to a worldwide audience might deface an e-commerce Web site, causing economic loss to the company arising from the inability to receive and process orders as well as reputational loss from the apparent security system breach that permitted the Web site vandalism. Finally, strategic information warfare might be executed to alter the strategic balance in an ongoing conflict. "A determined adversary could undertake a comprehensive, systematic effort to undermine U.S. military forces by compromising the commercial technologies and services that support them. Such an adversary could be ambitious and aim at nothing less than changing the strategic balance."[125]

Defending against Information Warfare

Mounting an effective defense to information warfare is a particularly daunting task because the apparatuses to carry it out are already widely available, and, indeed, many of the tools are employed daily for entirely legitimate purposes. In addition, these technology devices can be easily manipulated to perpetrate hostile attacks while leaving very little in the way of "fingerprints" to detect the origin of the attack and the responsible parties. For example, in many denial of service attacks, the individual originating the attack usually "spoofs" the source of the intrusion, giving the appearance that it was initiated in a different location. Therefore, because knowledge truly is power in the digital age, the first step in any defense planning against information warfare is educating the public about the very real dangers that exist with these new technology weapons. Although this seems a straightforward solution, observers speculate that the biggest obstacle to averting information warfare will be actually convincing individuals, governments, and industries to examine critical functions and processes with an eye toward securing them against information warfare attacks. Current practices in each of these segments virtually invite attacks due to

> poorly designed software applications; the use of overly complex and inherently unsecure computer operating systems; the lack of training and tools for monitoring and managing the

> telecomputing environment; the promiscuous inter-networking of computers creating the potential for proliferating failure modes; the inadequate training of information workers; and the lack of robust processes for identification of system components.[126]

In its task force report, the CSIS recommended that, after explaining the threat in terms that clearly articulate and emphasize its seriousness, the United States should develop national security policies designed to address the unique systemic vulnerabilities that arise from an interconnected and interdependent network infrastructure. According to the CSIS, this national policy should take the form of an executive order that precisely characterizes the nature and likelihood of strategic information warfare and that requires

> a top-down review of existing [governmental] organizations assigned responsibilities related to [information warfare], information security, security policy, and cybercrime. The review should result in recommendations ensuring that organizations' roles are consistent, do not overlap, and do not leave gaps and specifying how and under what conditions they will interface with each other.[127]

The CSIS also recommended that incentives be offered to the private sector to encourage the development and implementation of measures that improve security against strategic information warfare and simultaneously provide a benefit to the global networked community.

Finally, U.S. military and intelligence policies must now be refocused on the new threat of strategic information warfare. Because America's military and intelligence strategies have historically been oriented toward traditional weapons of war, the new focus must take into account that the modern threat will likely be launched over buried fiber-optic cables rather than experienced as land- or sea-based assaults. This revamping will require additional personnel with the requisite technical expertise, as well as significant collaboration with the private sector, whose participation will be critical to the creation and coordination of a national defensive approach to protect against strategic information warfare.

Congressional initiatives will also play an instrumental role in the battle against cyberterrorism, and, indeed, Congress has already acknowledged its responsibility to establish laws that take a proactive approach to this innovative form of terrorism. For instance, in January 2002, Senator John Edwards introduced two pieces of legislation designed to increase security and overall protection for the U.S. technology infrastructure. The Cyberterrorism Preparedness Act of 2002 would create a nonprofit consortium of academic and private sector experts to establish a set of "best practices" for the technology industry in an effort to effectively guard against cyberterrorism. According to the proposed legislation, *best practice* means

> a computer hardware or software configuration, information system design, operational procedure, or measure, structure, or method that most effectively protects computer hardware, software, network, or network elements against an attack that would cause harm through the installation of unauthorized computer software, saturation of network traffic, alteration of data, disclosure of confidential information, or other means.[128]

Contemplating that government implementation of best practices security systems will be the archetype for private industry and citizens alike, the act proposes that, after an initial assessment period, a report be created that identifies appropriate cybersecurity best practices that are reasonably susceptible to adoption by departments and agencies of the federal government over a two-year period. Such practices must permit customization or expansion of hardware, software, and network infrastructure, while taking into account the risk and magnitude of harm threatened by potential attack, the cost of imposing security protection, and the rapidly changing nature of the technology. Based upon that report, demonstration projects will be initiated to test the efficacy of the practices, and those deemed "security-enhancing, missions-compatible and cost-effective" will be implemented by the government forthwith. A separate but related bill, the Cybersecurity Research and Education Act of 2002, contemplates funding new Information Assurance fellowships to attract and train more researchers and teachers of cybersecurity.

On the international front, a draft report by NATO's Science and

Technology Committee entitled "Information Warfare and International Security" recommends that, due to the open and global nature of the Internet, laws regulating infrastructure protection and security should involve computer security experts and legislators internationally. The report also stresses the need for a symbiotic relationship between public and private entities because "[o]ften the private sector can better identify, understand and evaluate threats" and the exchange of information could be instrumental in detecting and preventing attacks on the infrastructure. Finally, the report raises a number of perplexing questions concerning the future impact of information technology on existing weapons systems, military organization, and strategy. For example, would it be possible to respond to an attack upon critical information systems with conventional forces and weaponry? Also, under what circumstances could a country deploy "offensive information warfare?"[129]

Ironically, during the Clinton administration, two Pentagon leaders proposed an "aggressive campaign of covert action against financial accounts and centers owned by al Qaeda." This clandestine operation called for U.S. operatives to acquire the necessary authentication to make valid withdrawals from terrorists' accounts, potentially "raining electronic havoc on a business or financial institution as a whole." However, then Treasury Secretary Robert Rubin vociferously opposed the plan, arguing that "as the world's preeminent financial center . . . the United States has the strongest interest in maintaining a global norm that cyberattacks on banking systems are acts of war. The United States could not defend that principle if it engaged in such attacks, and its own vulnerabilities would be substantial."[130]

In the short term, the threat of strategic information warfare as the preferred method of facelessly engaging and potentially destroying the enemy in modern times raises one key question for the United States: "Should [we] invest [our] shrinking defense dollars exclusively in additional fighter-bombers, carrier battle groups, and 70-ton tanks if the nation's most pressing vulnerabilities lie in its commercial information systems?"[131] Whether the United States can successfully defend against strategic information warfare depends upon its ability to spread the message that the threat exists and to marshal resources nationally and internationally to develop cost-effective polices to protect national security. Until then, the risk persists and evolves in dangerous lockstep with the global digital revolution.

The Continuing al Qaeda Threat

It remains unclear as of this writing, two years after the September 11 attacks, whether Osama bin Laden is dead or alive. He has not been apprehended. Mullah Omar, the former leader of the Taliban, has also escaped capture. However, after the decisive defeat of his forces by the coalition of Northern Alliance, American, and British troops and the evaporation of his Taliban during the Afghan campaign, he no longer poses the continuing threat to the United States that the remnants of the al Qaeda terrorist network do.

Although al Qaeda's headquarters and training camps have been destroyed and many of their top- and mid-level leaders captured, the group is still very active and carrying out terrorist strikes, reorganizing cells in the West and Middle East, and even negotiating new contacts with other terrorist organizations such as Lebanese-based, mostly Shiite Hezbollah. The Bush administration recognizes this continuing threat.[132]

Almost one thousand al Qaeda operatives have been arrested in sixty countries around the world, seriously disrupting its network; however, the threat continues. In testimony before Congress, CIA director George Tenet warned that "[o]perations against U.S. targets could be launched by al Qaeda cells already in place in major cities in Europe and the Middle East. Al Qaeda can also exploit its presence or connections to other groups in such countries as Somalia, Yemen, Indonesia and the Philippines. I must repeat that al Qaeda has not yet been destroyed."[133]

Nor are the various components of al Qaeda and their allies completely isolated incommunicado. They make use of a Codan radio network, like that used by UN and foreign aid workers in remote places. The recount of how an American rocket attack against al Qaeda forces in 2001 failed illustrates this radio network's importance:

> One night at the end of October, Osama bin Laden and 120 bodyguards came to spend the night at the camp of Beni

> Hissar, near Kabul. He told the camp boss that he would leave at eight the next morning. But he got up at five, prayed and then left. After that, everyone else was ordered out on the news that a missile attack was imminent. The rockets struck at eight. Since missile strikes happen with little or no warning, Mr. bin Laden evidently has some very reliable sources of information. The best of these, operated by his legion of foreign supporters, is linked by a sophisticated Codan radio network. . . . Arab and Afghan residents of Beni Hissar were given frequent warnings, via this network, of possible strikes by aircraft.[134]

Domestically, al Qaeda remains a threat as well. According to Attorney General Ashcroft, al Qaeda operatives posing as tourists, businessmen, and students are actively attempting to penetrate our borders. This is in addition to the already present "sleeper" cells that are plotting future attacks. Ashcroft explains:

> Today the United States is at war with a terrorist network operating within our borders. Al Qaeda maintains a hidden but active presence in the United States waiting to strike again. . . . There remain sleeper terrorists and their supporters within the United States who have not yet been identified in a way that will allow us to take pre-emptive action against them.

Federal officials say that many of these people are to be found in large cities, using the local Muslim community for support, to recruit sympathizers, and for cover.[135]

Table 1 illustrates foiled al Qaeda or al Qaeda–sponsored missions undertaken after September 11. Thus, we are faced with an enemy that not only continues to haunt us in our darkest nightmares but also continues to manifest itself through violent acts against civilians. The fluidity of its actions, flexibility of its remaining organization, secrecy of its planning and operations, and boldness of its deadly strikes make al Qaeda one of the toughest adversaries this country has faced. Nonetheless, it is, like every other adversary, defeatable in the end.

While America must reorganize its government, retool its mili-

TABLE 1. Foiled al Qaeda or al Qaeda–Sponsored Missions after September 11, 2001

Sept. 13, 2001	A Frenchman of Algerian background arrested in Paris said he had been part of a plot by Osama bin Laden to destroy the U.S. Embassy in Paris.
December	A Sudanese man with possible links to al Qaeda fired a Stinger missile at a U.S. warplane near Prince Sultan Air Base in Saudi Arabia.
December	Authorities in Singapore arrested thirteen suspected al Qaeda operatives and said they were part of a sleeper cell preparing to blow up several embassies.
December 22	Passengers and crew aboard an American Airlines flight from Paris to Miami subdued Richard C. Reid, who had the explosive C-4 in his shoes. Reid was linked by French authorities to Zacarias Moussaoui and al Qaeda.
January 2002	*Wall Street Journal* reporter Daniel Pearl was killed by Islamic militants, who kidnapped him in Karachi, Pakistan. The architect of the plan, Ahmad Omar Saeed Sheikh, has been linked to al Qaeda. He was arrested by Pakistani police, tried for the murder, and sentenced to death.
January	U.S. and Bosnian intelligence agencies captured an al Qaeda suspect who had planned attacks on U.S. bases, including Eagle Base outside Sarajevo.
February 20	The Italian police arrested four Moroccans with nine pounds of cyanide and a map pinpointing the location of the water pipes that lead to the U.S. Embassy in Rome.
March 17	Five worshipers, including an American embassy employee and her daughter, were killed when a man detonated a bomb in a Protestant church in Islamabad, Pakistan.
April 1	Seventeen people, including twelve German tourists, were killed in a synagogue bombing in Djerba, Tunisia. German and French investigators blamed al Qaeda, a spokesman for which, Sulaiman bu Ghaith, later claimed responsibility.
May 8	U.S. authorities arrested Jose Padilla, an American citizen who had trained in al Qaeda camps, as he traveled from Pakistan to the United States. Officials said he planned to detonate a radioactive bomb in the United States.
May 8	A Toyota Corolla exploded outside the Sheraton Hotel in Karachi, killing fourteen people, including eleven French citizens. French officials were "80 percent" certain al Qaeda was behind the attack.
June 11	Moroccan authorities announced they had broken up an al Qaeda cell that was planning to target NATO ships in the Strait of Gibraltar.
June 14	A vehicle loaded with explosives crashed into a guard post outside the U.S. Consulate in Karachi, killing eleven people and wounding twenty-six. American and Pakistani officials have yet to draw an al Qaeda connection, which they consider likely.
July 27	Mohammed Mansour Jabarah, an al Qaeda member and Canadian citizen, is arrested in Oman. He admitted directing his cell's unfulfilled plots to blow up the U.S. Embassy in Singapore as well as to attack other Western embassies, naval vessels, companies, and shuttle buses.

Source: New York Times. Data from FBI, CIA, and the Associated Press. Additional information compiled from *Time,* CNN, ABC News, MSNBC, *Financial Times, Chicago Tribune, Washington Post, Boston Globe,* and *Omaha World-Herald.*

tary, and reenergize its intelligence capability to fight this war, it can still be won without sacrificing our cherished way of life, basic freedoms, or fundamental civic convictions. The United States need not upset the balance of power nor sacrifice its democratic principles to win. It is precisely *because* we are America that we, perhaps uniquely in the world, can do both.