



CHILDREN AND FAMILIES
EDUCATION AND THE ARTS
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INFRASTRUCTURE AND
TRANSPORTATION
INTERNATIONAL AFFAIRS
LAW AND BUSINESS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
TERRORISM AND
HOMELAND SECURITY

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis.

This electronic document was made available from www.rand.org as a public service of the RAND Corporation.

Skip all front matter: [Jump to Page 1](#) ▼

Support RAND

[Browse Reports & Bookstore](#)

[Make a charitable contribution](#)

For More Information

Visit RAND at www.rand.org

Explore the [RAND Corporation](#)

View [document details](#)

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND electronic documents to a non-RAND website is prohibited. RAND electronic documents are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see [RAND Permissions](#).

The Tenth Year

A Briefing on Terrorism Issues to New Members of the 112th Congress

Brian Michael Jenkins

This product is part of the RAND Corporation corporate publication series. Corporate publications describe or promote RAND divisions and programs, summarize research results, or announce upcoming events.

Preface

On January 8, 2011, Brian Michael Jenkins, Senior Advisor to the President of the RAND Corporation, along with the Honorable Juan C. Zarate, former Assistant Secretary of the Treasury and Deputy Security Advisor for Combating Terrorism, briefed newly elected members of Congress. The briefings were designed to expose new members to a spectrum of foreign policy, national security, and domestic issues. The briefing was delivered twice, followed by discussions with individual members. Unlike formal congressional hearings, the sessions were deliberately informal. No written testimony was required, and no transcripts were made. This paper presents the gist of Jenkins's remarks.

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND focuses on the issues that matter most, such as health, education, national security, international affairs, law and business, and the environment. As a nonpartisan organization, RAND operates independently of political and commercial pressures. We serve the public interest by helping lawmakers reach informed decisions on the nation's pressing challenges.

The Tenth Year: A Briefing on Terrorism Issues to New Members of the 112th Congress

Brian Michael Jenkins

In America, terrorism time follows a 9/11 calendar. Everything that happened before is the pre-9/11 era, which most Americans only vaguely recall. It is important to remember, however, that America dealt with terrorism abroad and at home long before 9/11 and that U.S. counterterrorism efforts have a more than 40-year history. The post-9/11 era began on September 11, 2001. We are currently in the tenth year of this era. Ten years seems a long time, especially for a nation not known for its patience.

America has not suffered further 9/11s, as many initially feared it would. On the other hand, few in 2001 imagined that, ten years later, the United States would still be threatened by the jihadist terrorist enterprise it invaded Afghanistan to destroy. America's effort to defeat and dismantle this global terrorist project while protecting itself against further terrorist attacks has become its longest campaign. It will go on.

By now, Americans should have a fair idea of where they are in the contest with al Qaeda and what they still face, allowing for the inevitable uncertainties. They should be assured that intelligence, the costs of which have more than doubled, is at least adequate, that sufficient resources are being devoted to security, and that those resources are being sensibly allocated to reduce, not eliminate, risks. Americans should be persuaded that the nation's security efforts are smart, that the security measures to which they are being subjected—for many, their only personal contact with the government—are essential, and that they are participants in, not victims of, security efforts. Above all, they should be assured that their rights are being respected.

The 112th Congress should conduct a fundamental review of the nation's responses to the threat of terrorism. That is the principal message of the briefing to its newest members. Such a review does not mean demobilizing homeland security or slashing budgets to save money. It means calmly estimating the terrorist threats we face instead of reacting to the latest event. It means realistically calculating risks. It means estimating how much the federal government spends overall on countering terrorism—not an easy task—and how it is spent. It means thoughtfully reviewing programs, not to reduce counterterrorist efforts but to make them sharper and more sustainable. A meaningful review will require thoughtful inquiry, not the podium-pounding and partisan finger-pointing that have, in recent years, contributed to national cynicism and apathy. It will require political leaders to ask not how we can increase security but what might be done to build a more resilient society and a political environment that discourages rather than encourages overreaction.

Our Terrorist Foes Are Operationally Weaker, but Their Determination Is Undiminished

The global jihadist terrorist enterprise inspired by al Qaeda continues to pose the most significant immediate terrorist threat. It is not easy to assess the jihadists' current strength. Intelligence is imperfect, and there are no front lines or other obvious metrics to measure progress. Terrorism is more a matter of perceptions than of numbers. More than nine years after 9/11, informed analysts still disagree about whether al Qaeda is weaker or stronger. Their differences reflect the fact that al Qaeda is many things: It is the banner carrier of a radical expression of faith, the author of an ideology of endless armed struggle. It is the center of a global network of like-minded fanatics, the instigator of a global terrorist campaign, a contributor to ongoing insurgencies in Africa, the Middle East, and South Asia. It has an active communication system, which is essential to its continued existence and relevancy, and it is supported by a host of online jihadists. It has become a conveyer of societal and individual discontents, a magnet and compass for the most violent jihadists. Each of these dimensions merits separate analysis.

Most observers would agree that undeniable progress has been made in degrading al Qaeda's operational capabilities. An unrelenting campaign beginning with the invasion of Afghanistan in 2001 has reduced the likelihood of al Qaeda being able to mount further attacks on the scale of 9/11, while unprecedented international cooperation has created a more hostile environment for terrorists. But although al Qaeda has not been able to carry out a large-scale attack in the West since 2005, this does not diminish the 2008 attack on Mumbai by Lashkar-e-Toiba or the smaller but still deadly attacks and near misses seen elsewhere, including the killing of 13 U.S. soldiers and wounding of 31 others by Army Major Nidal Hasan at Fort Hood, Texas.

As a consequence of continuing pressure, the global terrorist campaign has become more decentralized, less dependent on direct support from al Qaeda's central command, which is now holed up somewhere in Pakistan. Although it remains in business, it is more dependent on local affiliates and allies that are not under its direct command and on its ability to inspire individual followers to violence.

The jihadist terrorist enterprise will morph according to its circumstances. Always opportunistic, it will attempt to exploit new grievances, join new conflicts. Over a very long term, its exhortations may become irrelevant, even to those it claims to represent, but it will not tire or be talked into submission.

Just three months after September 11, 2001, I was asked at a Senate hearing if we were "through it yet." Though seemingly premature, the optimism reflected in the question proved to be justified. America has suffered no more 9/11s, despite the patent ambitions of its terrorist foes to deliver another blow. But to destroy the terrorist enterprise, I thought then, would take many years. Ten years later, that remains the operative presumption.

Jihadist Terrorist Strategy Puts Increased Emphasis on Homegrown Terrorism

Terrorist training camps still exist in Pakistan and Afghanistan, some reportedly run as independent enterprises where volunteer operatives of different organizations commingle. Would-

be jihadists from Germany, England, Canada, and other Western countries also go to the camps for training, then return to their home countries to carry out attacks.

More than 20 of America's homegrown terrorists, including the failed Times Square bomber, received some type of terrorist training abroad. At least another 30 left the United States to seek terrorist training.

Authorities track communications and movements more closely now, making it harder to get Western would-be terrorists into and out of Pakistan. The training camps themselves are targets of missile strikes. At the same time, the terrorist organizations must be especially wary of Western infiltrators.

Faced with these difficulties, al Qaeda now places increased emphasis on do-it-yourself terrorism, urging local would-be jihadists to do whatever they can wherever they are. Without experience or practical instruction, homegrown terrorists have not achieved the sophistication of centrally supported efforts, but they have learned that attacks at home, even when unsuccessful, still cause great alarm. They boast that their attacks require little investment but bring high returns in terror while obliging governments to divert ever more resources to security. Their aim is to bleed America on foreign battlefields and bankrupt it with security requirements at home. Local attacks also draw suspicion to local Muslim communities, thereby contributing to their sense of isolation and persecution, which facilitates further terrorist recruiting.

The United States is not immune to the phenomenon of homegrown terrorism. According to a recent study by the RAND Corporation, between September 11, 2001, and the end of 2009, there were 46 known cases of Americans attempting to join jihadist terrorist groups abroad, providing them with material assistance, or plotting attacks to be carried out in the United States or other countries.¹ Most of the cases involved isolated, one-off attacks, unconnected to one another. Fortunately, the number of homegrown terrorists is small: 125 have been arrested or indicted over a period of more than eight years—a very small fraction of the estimated 3 million American Muslims. Apart from an ongoing recruiting effort targeting Somali immigrants, there is little evidence of continuity and certainly no evidence of any vast jihadist underground.

The year 2009 saw an increase in homegrown terrorism, with 13 cases involving 42 persons. It is still unclear whether this was a spike or a trend—in 2010, there were 11 cases involving 29 persons, fewer than in 2009 but more than twice the annual average between 2001 and the end of 2008.²

The small numbers defy quantitative analysis. Those arrested vary widely in age, economic status, education, and life experience. Their average (and median) age is 29. Almost all are U.S. citizens or legal permanent residents. The majority come from families that emigrated from North Africa, the Middle East, or South Asia. Somalis and Pakistanis are heavily represented, but the group includes U.S.-born Muslim converts. Some are dropouts, while others have advanced university degrees. Several have served in the armed forces. Others have criminal records—mostly for petty crimes. As terrorists, most were barely competent. Their plans and their performance were amateurish; nevertheless, it is important to point out that

¹ Brian Michael Jenkins, *Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001*, Santa Monica, Calif.: RAND Corporation, OP-292-RC, 2010.

² These were preliminary figures. Continuing research and a different breakdown of the clusters show 18 cases in 2010, involving 36 persons, although seven of these were the subject of previous indictments, leaving 29 new names, as indicated.

individuals who are not very smart can still be lethal. And some of those arrested were dangerously knowledgeable.

How effective homegrown terrorists can be also depends on how Americans as a society react. America's hyperactive, always hungry news media tend to exaggerate the drama of every event. Investigators and prosecutors, justifiably proud of intelligence successes and anxious to demonstrate that they are doing exactly what the public demands—prevent terrorist attacks—are reluctant to diminish the imminent threat posed by those arrested for fear of playing into the arguments of defense attorneys or losing popular support and government resources. In the highly partisan atmosphere of contemporary American politics, terrorist plots provide opportunities on both sides to score political points. Terrorists watch the spectacle, satisfied with the results.

Terrorist Campaigns Challenge All Democracies

Faced with the threat of terrorism, all democracies have felt obliged to facilitate intelligence collection, increase police powers, create new antiterrorist laws, toughen penalties for terrorist-related crimes, and, in some cases, alter trial procedures. Some countries have gone further, imposing censorship on the news media and suspending other civil liberties.

Pressure to change the rules is greatest in the immediate wake of a terrorist attack, when intelligence is seen to have failed, perceptions of risk are distorted by fear and alarm, and governments feel the need to be seen doing something. This can lead to hasty legislation and ambitious reorganization undertaken without fully considering the consequences. It makes more sense to consider sensitive issues during periods of calm, but then, of course, there is less perceived need to do so.

Since the traumatic attacks of 9/11, the United States has navigated a middle course. Congress passed legislation reorganizing the national intelligence effort, made information-sharing a priority, revised the electronic-surveillance law to reflect technological developments while maintaining the requirement of a judicial warrant, and created the Department of Homeland Security (DHS), endowing it with increased resources to insure against further terrorist attacks, all the while supporting wars in Afghanistan and Iraq.

However, it rejected the creation of a separate agency for domestic intelligence, warrantless surveillance, preventive detention, and the establishment of special courts to try Americans charged with terrorist crimes, while recognizing the necessity of special tribunals for trying those apprehended abroad and currently held at Guantanamo.

Conflicting American Attitudes Complicate Counterterrorism

American attitudes toward the terrorist threat seem to have become more ambivalent with the passage of time since 9/11. Without a major attack on American soil or on Americans abroad, the public has been sliding toward a dangerous complacency. There have not been this many consecutive years without a major terrorist incident involving American victims since the early

1970s.³ (This is not to diminish the tragic deaths of 13 people at Fort Hood or of those Americans killed by terrorists abroad since 9/11.) But this complacency is fragile, easily cranked up to apprehension. One terrorist attack, even a close call, can violently alter perceptions. Part of the problem is expectations.

Americans are, in fact, less exposed to violence today than they were in past decades. The country suffered far greater casualties in the wars overseas during the previous century than it has in Iraq and Afghanistan. It experienced much higher levels of criminal violence in the 1980s and 1990s and higher levels of domestic terrorist violence in the 1970s than it has since 9/11. Yet Americans' expectations of security appear to be greater now than ever before. Americans expect wars to be fought with zero casualties. They expect to live in a risk-free environment. This is unrealistic.

While demanding absolute security, Americans remain suspicious of their government. They have become cynical about the government's terrorist alerts. Willing to share remarkable amounts of personal information on vast social networks, they reject government infringement on their privacy. There is anger at irksome security measures. But if we accept the premise that the country is at war with tenacious terrorist foes, determined to attack American targets, we cannot feign shock and outrage when those foes carry out an attack, any more than a soldier on the front line could go into combat expecting not to be shot at.

Is Domestic Intelligence Adequate?

Domestic intelligence is always a delicate issue in a democracy. Although no large-scale terrorist attacks have occurred in the United States since 9/11, many jihadist terrorist plots have been uncovered and foiled, often as a result of domestic intelligence efforts. That is an intelligence success. Fortunately, the incompetence of most homegrown terrorists has given investigators some easy victories. (Critics charge that many of those arrested in these plots should not even be considered terrorists, arguing that they were simple-minded dupes snared by overzealous intelligence agents.)

Infiltrating terrorist conspiracies, identifying and heading off future terrorist attacks, and building the knowledge base to rapidly investigate terrorist incidents that do occur require human intelligence. That means recruiting and deploying confidential informants backed

³ The 1970s began with the political crisis caused by the hijacking of multiple passenger airliners by Palestinian extremists and ended with the seizure of hostages at the American Embassy in Tehran, setting off a protracted political crisis. In response, the United States threatened military action to end the 1970 hijacking crisis and attempted a military rescue of the hostages in Iran, which ended in failure.

The 1980s witnessed the bombing of the American Embassy in Beirut, killing 60; the bombing of the American Marine Corps barracks in Beirut, killing 240; the continuing hostage crisis in Lebanon; and the sabotage of Pan Am 103, killing 270. The United States again contemplated military action after the Marine Corps barracks bombing and, in 1986, bombed Libya in response to a Libyan-sponsored terrorist campaign.

The 1990s brought the first World Trade Center bombing in 1993, in which more than 1,000 people were injured; the 1995 Oklahoma City bombing, which killed 168; the 1998 suicide bombings of American embassies in Africa, in which hundreds of people died; and the suicide bombing of the USS *Cole*, in which 17 American sailors were killed.

The 9/11 terrorist attacks dwarfed all preceding events, but the subsequent decade so far has been remarkably quiet except for the Fort Hood incident.

up by trained undercover agents. It also means building trust with local communities and diasporas.

Despite the expansion of the Joint Terrorism Task Forces, combining federal authorities and local police, and the proliferation of fusion centers at the state and local levels, some experienced senior intelligence officials believe that the United States still lacks a coherent national domestic intelligence collection effort. There is no national estimate of domestic terrorist threats, no national domestic intelligence plan, no national domestic intelligence requirements, no priorities, no national coordination. Without greater central direction, a national domestic intelligence collection effort seems unlikely to emerge.

Central direction does not mean replacing the FBI with an American version of Britain's MI-5, and it certainly does not mean yet another disruptive reorganization of the intelligence community. But the idea of an integrated national intelligence enterprise that would be wholly owned and operated by state, local, and tribal law enforcement, with federal participation and assistance, is compatible with the nation's political traditions, although how this might emerge or operate in the absence of some central direction is not clear.

Local police are best positioned to collect intelligence about their own communities, as they do now about criminal gangs, but they lack resources and training, and few local departments offer career paths to reward those who develop the specialized skills and experience necessary to manage intelligence collection.

DHS views the country's 72 fusion centers as venues for receiving and sharing information passed down by the federal government. Very few fusion centers collect intelligence on their own, and they were not intended to do so. Their capabilities to analyze intelligence are limited. With state and local governments strapped for cash and federal spending constrained, some of the fusion centers may not survive.

DHS has shied away from taking charge of domestic intelligence collection while making itself the champion of information-sharing. Its rhetoric sometimes implies that information-sharing—connecting the dots, to use that now well-worn phrase—will by itself prevent future terrorist attacks. Critics see the emphasis on information-sharing as a deliberate diversion from the politically more sensitive task of intelligence collection.

Information-sharing has improved. DHS has greatly improved the flow of information down to the fusion centers and, indirectly, to local police departments. The flow upward has not been as smooth, and more information needs to be shared laterally. However, most fusion centers do not talk to one another, and differences in state rules for the handling of confidential information discourage its exchange.

While some may worry that the job of collecting domestic intelligence is not being done well enough, civil libertarians are alarmed by the growth since 9/11 of a vast enterprise that includes federal agencies—both the FBI and the Department of Defense, DHS, fusion centers, and local authorities, with significant involvement by private contractors, all devoted to domestic spying. While remaining suspicious of any domestic clone of the Central Intelligence Agency, they also worry that, without central management, the proliferation of participants, many poorly trained, and the consequent growth of databases recording ill-defined suspicious activity and the names of persons who have committed no crimes will get out of control and inevitably lead to the same kinds of abuses that occurred in the late 1960s and early 1970s.

There should be no illusion that this debate can be resolved through skillful legislation, and the continuing tension is not unhealthy in a democracy. Congress, however, can ask whether domestic intelligence collection is adequate. Is it capable of dealing with smarter adversaries?

Where should investments be made? How much intelligence collection is, or should be, in private hands? Is it being done properly, with appropriate monitoring and controls?

Should the Government Assert More Control Over the Internet?

Al Qaeda wants to build an army of believers, and its second-in-command, Ayman al-Zawahiri, has said that communication is 90 percent of the struggle. Terrorists have effectively exploited the Internet to spread their message to a global audience, without interference by censors or editors; to attract recruits; to exhort others to act; to provide them with practical instruction in the tactics and techniques of violence; and to clandestinely communicate with one another. According to a Saudi security official, al Qaeda now does 99 percent of its recruiting online.

The volume and quality of al Qaeda's communications have improved, even as its operational capabilities have declined. Its spokesmen—native-born Americans—appeal to an American audience. Its leaders regularly issue statements, and hundreds of English-language websites transmit the call for armed jihad. Slick online magazines offer firsthand accounts of manly adventures and provide bomb-making instructions. We are only beginning to comprehend the consequences of this communication.

The Internet is the starting point for many homegrown terrorists. (Some would argue that, given this incessant incitement to violence from abroad, it is incorrect to use the term *homegrown* terrorist.) At a minimum, it gives jihadist voyeurs a sense of participation, the safe thrill of vicarious jihad, and a fantasy world of belief, danger, power, and status—a violent video game. The Internet also enables extremists to find resonance and reinforcement for their personal discontents, provides them with direction, and justifies their aggression. Why, then, should government not assert more direct control over the Internet, outlawing incitement to terrorism as it now outlaws child pornography and other forms of online crime? Americans have tolerated censorship during times of war. What is different now?

The issue has come up before Congress several times. Limiting Internet communication would, opponents argue, be a blow to freedom, a terrorist victory. More practically, taking control of the Internet would require a significant policing effort. Those same resources might be better employed elsewhere. Most pragmatic is the argument that shutting down terrorist websites and chat rooms would deprive the authorities of a valuable source of intelligence. In fact, a number of terrorist plots have been foiled by monitoring communications on the Internet.

The United States needs to improve its capabilities in cyberspace, develop effective ways to blunt al Qaeda's appeal, and increase the awareness of family members and community leaders of the problem of online radicalization and recruitment to terrorism, but it should avoid imposing government control.

How Should the Government Allocate Finite Resources for Homeland Security?

Vulnerabilities in an open, technology-dependent society are virtually infinite. Resources are finite, even to meet the government's primary mission of providing for the common defense. If America were engaged in a traditional war, with a foreseeable end, the country could mobilize

to win and be done with it. But the struggle against terrorism is a continuing conflict for which risks and resources will have to be managed.

Some find the concept of risk management objectionable when applied to security against terrorist attacks, arguing that prevention must be the criterion for performance. But prevention is a goal—it is not a realistic criterion.

Americans need to be more savvy about risk. The threat that terrorists pose is a threat to society. Although a successful attack can result in significant loss of life, cause significant damage and economic disruption, arouse fear and alarm, and create political crises, the danger to any individual citizen is minuscule, far less than the risk we face on the highway.

Managing risks and resources does not call for a strict application of cost-benefit analysis. Terrorist attacks occur very rarely, although they have potentially serious consequences. That makes it difficult to measure the return on specific security investments.

Without inventing phony metrics or pretending that smart mathematical formulas can displace sound judgment, we need to develop databases, analytical approaches, and decision-making aids that help guide the allocation of limited resources. This is one of DHS's most important research tasks. And members of Congress have to stop viewing spending on homeland security as a bottomless pork barrel. The objectives are effectiveness and efficiency, not equity.

Is It Time to Rethink Aviation Security Strategy?

Despite some cynicism that airline security is a joke, over the long run, security measures aimed at reducing the number of terrorist hijackings and bombings appear to have worked, at least as a deterrent. Since the 1970s, when passenger screening was first introduced, the number of attempted airline hijackings and bombings has declined continuously. At that time, attacks on airliners were occurring at an average of one a month. By the 1990s, the annual average had dropped to four. Since 9/11, no airline hijackings have been attempted by terrorists, although several attempts have been made by mentally disturbed persons who had no weapons.

And despite occasional bad publicity, today's TSA screeners are a vast improvement over the pre-9/11 contract guards. However, increasing passenger loads and the continuing addition of security procedures (requiring passengers to remove shoes in 2001, restriction on liquids in 2006, the deployment of body scanners in 2010) will create growing stress, which could degrade performance.

Obsessed with attacking aviation, terrorists are constantly developing new ways to evade detection or defeat security measures. Finding bombs has always been difficult, and it represents the biggest challenge today. At the turn of the 21st century, terrorists had a better than 50-percent success rate in getting bombs on board aircraft. All six known attempts to smuggle bombs into passenger cabins since 9/11 succeeded, although only three devices actually exploded.

The good news is that security measures appear to be forcing terrorists to design more concealable explosive devices that use smaller quantities of explosives and less reliable detonating mechanisms. The devices can be smuggled on board, but they are less likely to work, and less likely to bring the plane down if they do. The bad news is that terrorists can construct and conceal bombs in ways that make them undetectable by all but the most intrusive searches. The recent protest against body scanners and the new pat-down procedures was greatly exag-

gerated, but it is nonetheless an indicator that measures to ensure security are at the edge of provoking those being protected. Security that becomes a matter of us-versus-them will not work.

In my view, current preboard screening is not adequately effective. What we have in place is not the result of design; rather, it is an accumulation of machines and procedures, each implemented in response to a specific event. It is time to consider an entirely different approach, one that places more emphasis on looking at individual travelers than on searching for objects.

Subjecting all airline passengers to the same security regime does not constitute intelligent security. The approach must be more discerning. Admittedly, many do not share this opinion. But either way, it is time to fundamentally review how airline security is provided.

Should More Resources Be Devoted to the Security of Public Surface Transport?

Devoting considerable resources to aviation security is understandable. It is not merely a reaction to the 9/11 hijackings, although that event drove the implementation of a number of significant changes. But as indicated by subsequent events—the attempted sabotage of an airliner by the shoe bomber in 2001, the 2006 Heathrow plot, the Christmas Day 2009 sabotage attempt by the so-called underwear bomber, and the attempts in 2010 to introduce bombs through air courier services—terrorists continue to be obsessed with attacking airliners. The threat is real.

Other security concerns are more the product of vulnerability assessment than of threat assessment. Competing for finite security resources, threat advocates champion specific vulnerabilities, drawing attention to the catastrophic consequences if terrorists were to successfully attack certain targets, but these scenarios are often hypothetical. This does not mean that the vulnerabilities are not real or that analysts should not try to anticipate things that terrorists might do.

The threat to public surface transportation is not hypothetical—it is well established in terrorist playbooks. Terrorists see trains and buses as easily accessible killing fields that offer opportunities to achieve high body counts, cause great alarm, and create costly disruptions. Three terrorist attacks on commuter trains and subways in Madrid, London, and Mumbai resulted in more than 450 fatalities and thousands of injuries.

Since 9/11, terrorists worldwide have carried out 74 attacks on airplanes and airports, causing 121 fatalities. But during the same period, 1,214 terrorist attacks on public surface transport killed 3,350 people.⁴ Since 9/11, four terrorist attempts have been made on aircraft heading for the United States. In the same period, U.S. authorities have uncovered six terrorist plots against subways and commuter rail systems. It can happen here, yet public surface transport receives only a small fraction of the federal funds devoted to aviation security. Although the amounts have increased in recent years, surface transportation security merits more attention.

⁴ These statistics were compiled by the Mineta Transportation Institute. For an earlier statistical analysis of attacks on surface transportation, see Brian Michael Jenkins and Bruce R. Butterworth, *Explosives and Incendiaries Used in Attacks on Public Surface Transportation: A Preliminary Empirical Analysis*, San José, Calif.: Mineta Transportation Institute, 2010.

Are Security Expenditures Untouchable?

Al Qaeda hopes that America will bankrupt itself fighting costly military wars overseas while burdening its economy with ever-increasing security measures at home until it collapses, as the Soviet Union did after years of fighting in Afghanistan. Terrorists know that they have an advantage. It is an axiom that the costs of security are determined less by the threat than by the size and number of targets to be protected.

One failed airline bomber obliges authorities to implement new security measures at hundreds of airports at a cost of hundreds of millions of dollars. It is a bad exchange. In addition to the direct costs, security measures can have insidious adverse effects on commerce that are not easily measured but impede the flow of people, goods, and ideas essential to a free economy.

If we accept the premises that this is the threat environment that America will live with for the foreseeable future, that security measures imposed now are likely to become permanent features of the landscape, and that a free society and economic strength are vital components of America's national security, our aim must be sustainability.

Rapid increases in spending on intelligence and homeland security were necessary in the dark days immediately after 9/11. In the shadow of a disastrous terrorist attack, uncertain of the enemy's capabilities or whether another attack was on the way, America went to war while preparing for the worst at home. Budgets were not the issue. All wars are wasteful. This one would be no exception.

Since that time, a tendency to view the security budget as untouchable has developed. But Congress cannot allow unreasonable fear and unrealistic demands for security to keep the wagon train circled forever. Speaking candidly, the time is right and the political circumstances are propitious. The majority party in the 112th Congress can conduct a thorough review of intelligence and homeland security without risking the criticism that a review by the previous Congress might have invited. The President has demonstrated his determination to take on the terrorists. There is an opportunity for a bipartisan approach.