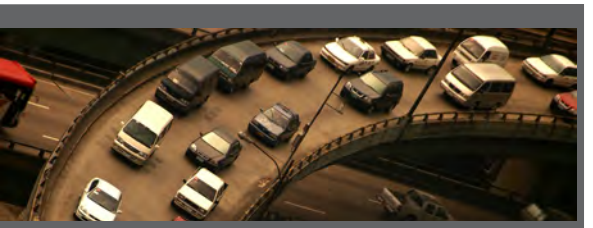
The Challenge of Protecting Transit and Passenger Rail: Understanding How Security Works Against Terrorism

MTI Report 12-74



MINETA
TRANSPORTATION INSTITUTE
MTI

MINETA TRANSPORTATION INSTITUTE
LEAD UNIVERSITY OF MNTRC

The Mineta Transportation Institute (MTI) was established by Congress in 1991 as part of the Intermodal Surface Transportation Equity Act (ISTEA) and was reauthorized under the Transportation Equity Act for the 21st century (TEA-21). MTI then successfully competed to be named a Tier 1 Center in 2002 and 2006 in the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU). Most recently, MTI successfully competed in the Surface Transportation Extension Act of 2011 to be named a Tier 1 Transit-Focused University Transportation Center. The Institute is funded by Congress through the United States Department of Transportation's Office of the Assistant Secretary for Research and Technology (OST-R), University Transportation Centers Program, the California Department of Transportation (Caltrans), and by private grants and donations.

The Institute receives oversight from an internationally respected Board of Trustees whose members represent all major surface transportation modes. MTI's focus on policy and management resulted from a Board assessment of the industry's unmet needs and led directly to the choice of the San José State University College of Business as the Institute's home. The Board provides policy direction, assists with needs assessment, and connects the Institute and its programs with the international transportation community.

MTI's transportation policy work is centered on three primary responsibilities:

Research

MTI works to provide policy-oriented research for all levels of government and the private sector to foster the development of optimum surface transportation systems. Research areas include: transportation security; planning and policy development; interrelationships among transportation, land use, and the environment; transportation finance; and collaborative labor-management relations. Certified Research Associates conduct the research. Certification requires an advanced degree, generally a Ph.D., a record of academic publications, and professional references. Research projects culminate in a peer-reviewed publication, available both in hardcopy and on TransWeb, the MTI website (http://transweb.sjsu.edu).

Education

The educational goal of the Institute is to provide graduate-level education to students seeking a career in the development and operation of surface transportation programs. MTI, through San José State University, offers an AACSB-accredited Master of Science in Transportation Management and a graduate Certificate in Transportation Management that serve to prepare the nation's transportation managers for the 21st century. The master's degree is the highest conferred by the California State University system. With the active assistance of the California Department of Transportation, MTI delivers its classes over a state-of-the-art videoconference network throughout the state of California and via webcasting beyond, allowing working transportation professionals to pursue an advanced degree regardless of their location. To meet the needs of employers seeking a diverse workforce, MTI's education program promotes enrollment to under-represented groups.

Information and Technology Transfer

MTI promotes the availability of completed research to professional organizations and journals and works to integrate the research findings into the graduate education program. In addition to publishing the studies, the Institute also sponsors symposia to disseminate research results to transportation professionals and encourages Research Associates to present their findings at conferences. The World in Motion, MTI's quarterly newsletter, covers innovation in the Institute's research and education programs. MTI's extensive collection of transportation-related publications is integrated into San José State University's world-class Martin Luther King, Jr. Library.

REPORT 12-74

THE CHALLENGE OF PROTECTING TRANSIT AND PASSENGER RAIL: UNDERSTANDING HOW SECURITY WORKS AGAINST TERRORISM

Brian Michael Jenkins

February 2017

A publication of
Mineta Transportation Institute
Created by Congress in 1991

College of Business
San José State University
San José, CA 95192-0219

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No. CA-MTI-1130	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle The Challenge of Protecting Transit and Passenger Rail: Understanding How Security Works Against Terrorism		**5. Report Date** February 2017 **6. Performing Organization Code**
7. Authors Brian Michael Jenkins		**8. Performing Organization Report** MTI Report 12-74
9. Performing Organization Name and Address Mineta Transportation Institute College of Business San José State University San José, CA 95192-0219		**10. Work Unit No.** **11. Contract or Grant No.** DTRT12-G-UTC21
12. Sponsoring Agency Name and Address California Department of Transportation Division of Research, Innovation and Systems Information MS-42, PO Box 942873 Sacramento, CA 94273-0001 U.S. Department of Transportation Office of the Assistant Secretary for Research and Technology University Transportation Centers Program 1200 New Jersey Avenue, SE Washington, DC 20590		**13. Type of Report and Period Covered** Final Report **14. Sponsoring Agency Code**

15. Supplemental Notes

16. Abstract

Terrorists see transit and passenger rail as an attractive target. Designed for public convenience, trains and stations offer terrorists easy access to crowds of people in confined environments where there are minimal security risks and attacks can cause high casualties. This report examines the unique attributes of the terrorist threat, how security measures against terrorism have evolved over the years, and their overall effectiveness.

Does security work? Empirical evidence is hard to come by. Terrorist incidents are statistically rare and random, making it difficult to discern effects. The fact that terrorists focus most of their attacks on targets with little or no security suggests that security influences their choice of targets. Increased security does not reduce terrorism overall, but appears to push terrorists toward softer targets. These indirect effects are visible only over long periods of time.

Public surface transportation poses unique challenges. It is not easy to increase security without causing inconvenience, unreasonably slowing travel times, adding significant costs, and creating vulnerable queues of people waiting to pass through security checkpoints. This has compelled rail operators to explore other options: enlisting passengers and staff in alerting authorities to suspicious objects or behavior, random passenger screening, designing new stations to facilitate surveillance and reduce potential casualties from explosions or fire, and ensuring rapid intervention.

17. Key Words Transportation; transit; trains; terrorism; security	**18. Distribution Statement** No restrictions. This document is available to the public through The National Technical Information Service, Springfield, VA 22161		
19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 65	**22. Price** $15.00

Form DOT F 1700.7 (8-72)

Library of Congress Catalog Card Number:
2017933311

To order this publication, please contact:

Mineta Transportation Institute
College of Business
San José State University
San José, CA 95192-0219

Tel: (408) 924-7560
Fax: (408) 924-7565
Email: mineta-institute@sjsu.edu

transweb.sjsu.edu

021317

ACKNOWLEDGMENTS

The author thanks MTI staff, including Executive Director Karen Philbrick, Ph.D.; Publication Support Coordinator Joseph Mercado; Executive Administrative Assistant Jill Carter; Editor Janet DeLand; and Webmaster Frances Cherman.

TABLE OF CONTENTS

I. INTRODUCTION

When active counterterrorist measures have not succeeded in destroying terrorist organizations and intelligence has failed to detect their plots, security measures constitute the last line of defense. But does security work against an adversary that poses such unique challenges? Empirical evidence is hard to come by. Terrorist incidents are statistically rare and random, making it difficult to discern direct effects. Security against terrorism seems to work primarily as a deterrent. The fact that terrorists focus the overwhelming majority of their attacks on "soft" targets that have little protection or carry out their attacks in ways that obviate security suggests that terrorists are deliberately avoiding better-protected targets. That itself is evidence that security has some effect on terrorist decisionmaking. Increased security does not reduce terrorism, but it appears to push terrorists away from some targets. However, these indirect effects are visible only over long periods of time.

Terrorism is intended to create fear—and it often works. Even small attacks cause significant alarm. As a result, an apprehensive public demands *absolute security*. But increased protection around terrorists' traditional targets has driven them toward more random, indiscriminate attacks—that is, *pure terrorism*. Today's terrorist organizations justify and encourage attacks such as mass killings and less-rational, unpredictable small-scale assaults, which are harder to prevent.

Continued terrorist interest in transportation targets was demonstrated in the March 2016 bombing of the metro in Brussels, in which 13 people died; the July 2016 knife and axe attack on train passengers in Wuerzberg, Germany, in which four persons were injured; and the discovery in October 2016 of an improvised explosive device on a London Underground train. Terrorists see transit and passenger rail as attractive targets. Designed for public convenience, trains, subways, and stations offer terrorists easy access to crowds of people in confined environments where attackers face minimal security risks and where bombings, shootings, and other types of attacks can cause high casualties. Terrorist attacks on widely used public transport also create significant alarm—daily commuters and other passengers cannot easily avoid what they perceive as a source of danger. At the same time, it is not easy to increase security without causing inconvenience, unreasonably slowing travel times, adding significant costs, and creating vulnerable queues of people waiting to pass through security checkpoints.

Designed for public convenience, trains, subways, and stations offer terrorists easy access to crowds of people.

This has compelled rail operators to explore other security options. These include enlisting passengers and staff in alerting authorities to suspicious objects or behavior, random passenger screening, designing new stations to facilitate surveillance and reduce potential casualties from explosions or fire, and ensuring rapid intervention and evacuation of people out of harm's way.

But do these—or any security measures against terrorism—work?

This report examines the terrorist threat, how security against terrorism has evolved over the years, and the overall effectiveness and specific effects of security measures on terrorist tactics and targeting.[1] It addresses five questions:

- How has terrorism evolved in recent years and what is the nature of the contemporary terrorist threat?
- How does terrorism differ from certain other forms of violent crime and from other modes of armed conflict—and what are the implications of these differences for security against terrorist attacks?
- How have the officials charged with security responsibilities in both the public and private sectors tried to protect against terrorist attacks?
- How well have security measures worked?
- Since physical security measures seldom catch terrorists like insects in a net, do security measures have a deterrent effect on terrorism?

Each of these questions brings up numerous additional questions. For example, How have terrorist tactics or the targets of terrorist attacks changed since terrorism emerged in its contemporary form in the late 1960s and early 1970s? How do the authorities decide on the allocation of their limited resources for security? This itself is a complex discussion with broader implications for how society reacts to terrorism. If terrorist attacks cannot all be prevented, can more be done to reduce the terror they are intended to create? How do terrorists try to overcome or obviate security measures put in place to stop them? Why do terrorists seem to succeed so often? Is it because security measures often fail? And If that is the case, how and why do they fail? Can the effectiveness of security measures be empirically evaluated? According to what criteria?

Can the effectiveness of security measures be empirically evaluated?

Even raising such questions risks ruffling some feathers, as they may be perceived as critical of government homeland security efforts or those of the security industry. Some may wrongly interpret this discussion as going soft on the security of the American people on grounds that it is futile or as a misguided attempt to mechanically apply cost-benefit analysis to the complex threat posed by terrorists. None of these are my intentions. The purpose of this report is to provide a better understanding of what can (and cannot) be achieved, at what cost.

Questions of costs and effectiveness were close to irrelevant in the immediate aftermath of 9/11. The United States had just suffered the worst attack in the annals of terrorism. More large-scale attacks were anticipated, with possibly even worse consequences. The perceived necessity was to do whatever the country could do to prevent another major attack. As time has passed, however, questions about America's response have arisen. Always pragmatists, Americans want to know not simply if they are safer—they are—but whether continued involvement in foreign wars and the significant security expenditures at home are prerequisites to keeping America safe.

The observations and conclusions presented in this report are drawn from research conducted over the past 20 years at the Mineta Transportation Institute (MTI) and from my work at other research institutions. But the report also reflects views developed from my personal experience over the past four decades as a member of or advisor to various national commissions on terrorism and as a consultant to law enforcement and the private sector.[2]

Security against terrorism can be defined broadly to include all measures aimed at reducing the terrorist threat overall while protecting society against terrorist attacks. In its broadest sense, security would include military efforts abroad to destroy terrorist organizations or at least degrade their operational capabilities, foreign and domestic intelligence collection, and law enforcement, augmented by physical security measures—the last line of defense. The U.S. Defense Department classifies these efforts either as "counterterrorism," comprising offensive measures against terrorist organizations, or "antiterrorism," comprising defensive measures to reduce the vulnerability of persons and property.[3] This report focuses specifically on antiterrorist or physical security measures. It excludes military operations against terrorist groups and efforts to resolve conflicts that may lead to terrorism or efforts to counter violent extremism, which are components of a broader strategy to combat terrorism. The report only touches upon the role of intelligence and more-active measures such as countersurveillance. It does, however, examine efforts to enlist the public in alerting authorities to suspicious activity.

Although they represent a narrower subset of efforts to counter terrorism, physical security measures include not only efforts to discourage attacks or prevent successful attacks, but also measures to reduce casualties and damage if an attack occurs. The latter include design and construction features to mitigate the effects of explosions and facilitate rapid response and evacuations. As a general observation, the difficulties of preventing terrorist attacks have pushed counterterrorism strategy upstream toward intervention *before* attacks occur and at the same time have caused those in charge of security to increase efforts aimed at mitigation, resiliency, rapid response, and speedy recovery *after* an attack.

Despite best efforts to stop them, determined terrorists will carry out attacks.

The role of physical security measures is limited—despite best efforts to stop them, determined terrorists will carry out attacks. Society can try to address the grievances that give rise to radicalization and recruitment, discourage or deflect individuals from becoming terrorists, intervene at the earliest possible indication of violent intentions, uncover and disrupt terrorist plots, prevent successful attacks or deter terrorists from attacking certain targets through physical security measures, design facilities in ways that will mitigate casualties, facilitate rapidly neutralizing any attack that occurs, and facilitate rapid recovery. Physical security measures are only one component of this sequence.

Increasing emphasis is now being placed on countering violent extremism. The results of this effort are not yet clear. Laws and procedures also have been changed to facilitate intelligence collection and allow authorities to intervene earlier—well before an attempted attack. This has opened a new domain in law enforcement and security between the first indications of criminal intentions and actual attempts to commit terrorist acts. In law

enforcement, it has allowed prosecution on the basis of intentions, which, in turn, has expanded the use of confidential informants and undercover police intelligence operations. This appears to have achieved some success.

Current research is exploring whether anything can be done in the narrower time frame between an attacker's final commitment to action and an actual attack. In other words, can we widen the last line of defense? At what point does an imminent attack become manifest? Behavior detection looks for indications of suspicious behavior. Are there subtle but visible clues in individual behavior indicating imminent attack that may be discerned by trained observers or by computerized real-time analysis of video surveillance? Such clues might take the form of unusual behavior—loitering in odd places or visibly avoiding security personnel at the scene of the intended attack. Theoretically, intentions could be tested through subtle prompts—an provocative image or a question that pops up on the screen at an airport check-in kiosk while facial expressions are monitored. This is a controversial new area where developments potentially could have profound consequences for security but also for the law and individual privacy.

ORGANIZATION OF THIS REPORT

The report begins with a description of the origins of contemporary terrorism and the major changes that have occurred. It examines the reason for the apparent dramatic increase in the volume of terrorist activity worldwide, the escalation of violence as terrorists have sought higher and higher body counts, the increasingly indiscriminate nature of terrorist violence as attackers kill in quantity or move toward totally random killing, the rise of suicide terrorist attacks, and the phenomenon of remotely inspiring and instructing distant supporters who are not physically in touch with a terrorist organization—so-called homegrown terrorists—to carry out attacks.

The next section looks at the ways in which terrorism differs from more-conventional modes of armed conflict and from certain forms of crime such as high-value armed robberies, and what these differences mean for security. Terrorists have the enormous advantage of virtually unlimited targets. Security does not prevent terrorism; it merely increases the chance of terrorist failure or displaces the risk to other, more-vulnerable targets—more often the latter. Unlike wartime commando raids or armed robberies, terrorist attacks do not require tactical success to be effective. Since terrorism is aimed at attracting attention and creating terror, even failed attempts can still cause alarm and oblige authorities to respond with new security measures that seem to validate public fears. This psychological dimension of terrorism is critical to the theory of terrorism itself, but it is often overlooked in society's responses.

Security does not prevent terrorism; it merely increases the chance of terrorist failure or displaces the risk to other, more-vulnerable targets—more often the latter.

The report next considers how much is spent on security against terrorism and what society expects the expenditures to accomplish. What antiterrorist strategies and approaches are used? What are the specific categories of security measures, what are they each intended to do, and how well do they work? This section also looks at some of the major developments in security over the years and explores the effects of these developments.

Measuring the effectiveness of security measures against terrorism turns out to be extremely difficult, as terrorism poses unique challenges that defy easy empirical evaluation. Terrorists can overcome almost all security challenges by changing their target sets. Their usual direction, and therefore the long-range trend in terrorist violence, is toward softer targets that are difficult, disruptive, and costly to defend. But this is not always the case: On some occasions, terrorists seem determined to go after harder targets even when easier targets are available, in order to defeat a challenge and display their determination and skill—thus creating more public fear.

Cost-benefit analyses of security can be performed, using fatalities and the economic costs of the damage and disruption to commerce caused by the terrorists as the criteria. But these analyses ignore the psychological dimension. The effect of a terrorist attack is not simply a matter of the number of deaths or the amount of destruction that results, it must also include the psychological effects on the terrorists' target audience. While the statistical risk to the individual is minuscule compared with the risk of other sources of mortality, the societal impacts of even modest terrorist attacks—whether the attacks are successful or not—can be significant.

While the statistical risk to the individual is minuscule...the societal impacts of even modest terrorist attacks...can be significant.

That would seem to make security against terrorism an almost futile undertaking; however, terrorists take security seriously, and some long-term effects of security are discernible. When faced with high levels of security, terrorists do alter their behavior. There is anecdotal and statistical evidence that security measures have a deterrent effect, which is examined later in the report.

Since much of the research discussed here pertains to surface transportation, the report offers some specific observations about the challenges faced by transportation security. In particular, it examines how terrorists view surface transportation as a target and what terrorist plotters think about specific security measures in that theater of their activity.

The report ends with some overall conclusions.

II. THE EVOLVING NATURE OF THE TERRORIST THREAT

Terrorist tactics have been used for centuries, but terrorism in its contemporary form emerged in the late 1960s and early 1970s. The phenomenon announced its arrival with a series of spectacular events, including a number of political assassinations and a rise in terrorist bombings. Assassinations and bombings had been part of the terrorist tactical repertoire for decades, but modern terrorists added some new tactics. The first airline hijacking with political demands occurred in 1968. Terrorists turned to multiple hijackings in 1970. The first kidnapping of a diplomat in order to make political demands occurred in 1969. The first politically motivated bombing of a commercial airliner took place in 1970. The first embassy seizure by terrorists took place in 1972. Ransom kidnappings by terrorists to fund their operations began in 1973.

No common cause connected the groups responsible for these early events other than a shared sense of failure and frustration that neither the mass protests nor the more traditional modes of guerrilla warfare that marked the political ferment of the 1960s had achieved success. Mao Zedong's concept of guerrilla warfare made the people, normally consigned to the sidelines of the battlefield in conventional warfare, an essential part of war-fighting strategy. Military operations had to have a political component to be justified—they had to appeal to the masses. Terrorism further elevated the role of the audience. The primary purpose of most terrorist operations was to affect perceptions. Terrorism was aimed at the people watching.

The primary purpose of most terrorist operations was to affect perceptions. Terrorism was aimed at the people watching.

Terrorists did not need to match the military capacity of their adversaries. Small groups with a limited capacity for violence could achieve disproportionate effects by carrying out spectacular acts intended to attract attention and cause people to exaggerate the terrorists' strength and inflate the perceived threat. The mere creation of terror enabled terrorists to achieve their political goals.

Technological developments also played a key role in the rise of modern terrorism. Modern technology-dependent society offered new vulnerabilities. Explosives could easily be acquired or fabricated. Expanding production produced volumes of firearms that made them a commodity like any other—hundreds of millions of individual firearms were circulating in the world, most of them in private hands. It is in the realm of communications, however, that technological developments most dramatically enhanced terrorist tactics. Radio, television, and communications satellites gave terrorists the ability to reach an audience of global proportions almost instantaneously, and this provided them with enormous power and great incentives.

TERRORISM HAS INCREASED IN VOLUME

Since 1970, terrorism has increased in volume and has become increasingly international. The Global Terrorism Database (GTD) maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland

recorded 157,522 incidents of terrorism, with a total of 351,428 fatalities, between 1970 and 2015. For 2015 alone, the GTD shows 14,807 incidents of terrorism worldwide (down from 16,804 incidents in 2014).[4] This compares with an annual average of 984 incidents in the 1970s; 3,116 in the 1980s; 3,058 in the 1990s; and 2,499 between 2000 and 2009.[5]

The dramatic increase in terrorism worldwide, however, is misleading. Outside of conflict zones, where terrorist campaigns comprise merely one aspect of ongoing wars, terrorist attacks occur only occasionally. Although terrorists carried out attacks in more than a hundred countries between 2001 and 2015, just ten countries accounted for 73 percent of all recorded terrorist attacks and 75 percent of all fatalities. This high proportion of terrorist activity reflects long-running insurgencies in Iraq, Pakistan, Afghanistan, India, the Philippines, Thailand, Nigeria, Somalia, Yemen, and Colombia. Forty-six percent of the incidents, accounting for more than 50 percent of the fatalities, took place in just three countries—Iraq, Afghanistan, and Pakistan—all of which were engulfed in intense ongoing armed conflicts.

Outside of conflict zones, where terrorist campaigns comprise merely one aspect of ongoing wars, terrorist attacks occur only occasionally.

This conforms to a general historical pattern. Only 14 percent of all terrorist attacks since 1970 have occurred in Europe. And if the data are confined to incidents with fatalities, the disparities between terrorism in and outside of conflict zones are even greater.[6]

Although it includes only attacks on surface transportation—a popular terrorist target—the database maintained by MTI confirms this pattern. Between 1970 and the end of 2015, MTI counted 3,409 attacks on buses, passenger trains, and ferries worldwide. The countries of South and Southeast Asia and the Middle East account for about 70 percent of this total. The MTI database excludes incidents in active war zones, although it does report terrorist attacks in Pakistan. If Afghanistan and Iraq were included in the MTI database, these regions would account for a much higher percentage of the total number of attacks. European countries plus the United States and Canada account for only about 10 percent of attacks worldwide during this 45-year period. Clearly, the developing world experiences far more attacks. Moreover, according to the MTI database, attacks in South Asia are three to four times more lethal than those in Europe.

The MTI database tracks the increase in terrorism worldwide along a trajectory similar to that seen in the GTD. The number of attacks trends upward from the 1970s to the turn of the century, then it levels off but remains well above the totals for the earlier decades. The GTD continues a sharper upward climb.

In other words, most recent terrorist incidents occur under conditions of armed conflict, i.e., ongoing wars. Terrorism increased from the 1970s on, but the dramatic increase in recent years is mostly a reflection of the fact that terrorism has become a distinguishable component of warfare and is now counted as a separate category of violence even during war. This makes historical comparisons and discerning long-term trends difficult. We have no idea how many incidents that would now be categorized as terrorist attacks occurred during World War II, the civil war in China, the Vietnam War, or the civil war in Lebanon—

presumably there would be many. The increase appears all the more dramatic because the incidence of warfare itself and the casualties produced by war have declined during the same period.

There are fewer wars and fewer casualties today than there were 50 years ago, and certainly fewer than there were in the bloody first half of the 20th century, when two world wars resulted in the deaths of approximately 5 percent of the world's population.[7] Terrorism looms larger, in part because warfare itself has diminished, but also because terrorists have carried out more-spectacular attacks.

Terrorism looms larger, in part because warfare itself has diminished, but also because terrorists have carried out more-spectacular attacks.

TERRORISTS HAVE ESCALATED THEIR VIOLENCE

In a world in which terrorist attacks were becoming increasingly commonplace, ever more spectacular acts of bloodshed were needed to achieve impact—increased terrorism created an inflationary effect that demanded terrorist escalation. The increasing role played by religious fanaticism as opposed to secular ideologies also drove terrorism into higher registers. Terrorists who claimed to be fighting for political goals—separate states or new societies—had to concern themselves with constituencies. Worries about alienating their claimed supporters imposed constraints on their violence. These self-imposed constraints eroded as terrorists escalated their violence in God's name, although even religious fanatics worried that going too far could provoke damaging backlashes.

New terrorist groups coming onto the scene seldom replicated the trajectory of their predecessors, who escalated from mostly symbolic to more-lethal attacks. The new terrorist groups did not start over at the bottom rung but began their campaigns using the most recent tactics and operating at the prevailing level of violence—they began with killings—and from there escalated even further than their predecessors. As a result, even though a number of the earlier terrorist groups were destroyed, the new, more-violent groups pushed the overall lethality of terrorist violence upward.

The GTD provides a sense of this escalation. In the 1970s, the average number of fatalities per terrorist incident was 0.72. This rose to an average of 2.19 fatalities per terrorist incident in the 1980s, which rose to 2.26 in the 1990s, and to 2.91 from 2000 to 2009, dropping back to 2.19 for the six-year period from 2010 to 2015.[8] While these increases seem slight, they represent a more than threefold increase in lethality.

A better idea of the escalation can be gained by looking at the incidents with the most fatalities. The bloodiest incidents of terrorism in the 1970s produced tens of fatalities. This ascended to hundreds of fatalities in the bloodiest terrorist incidents in the 1980s. On September 11, 2001, the number ascended to thousands of fatalities. This represented an order-of-magnitude increase every 15 years, leading to post-9/11 extrapolations that forecast future terrorist use of weapons of mass destruction, enabling them to kill tens of thousands or even hundreds of thousands of people.

TERRORISTS NOW KILL MORE INDISCRIMINATELY

Killing in quantity means killing indiscriminately. As time went on, terrorists defined their enemies—and therefore those they considered legitimate targets—more broadly. This also turns out to be an easy way around security measures. Today's terrorists are approaching what might be called "pure terrorism," totally random violence, killing *anyone*—people dining at a restaurant, gathered to watch fireworks or a concert, or at a busy intersection—in order to make a political point. Blowing up or gunning down people at cafes is not entirely new. It is, however, increasingly the norm.

Today's terrorists are approaching what might be called "pure terrorism," totally random violence.

TERRORISTS ARE MORE WILLING TO DIE CARRYING OUT THEIR ATTACKS

The emergence of suicide attacks started another trend. Suicide attacks were a response to increased security and were intended to be a demonstration of fanatical commitment, which itself would cause fear. Initially employed by only a handful of groups, reflecting specific cultural norms or the creation of suicidal subcultures to imitate the assassins of the 11th century, the use of suicide attacks soon became widespread.

The GTD records the first terrorist suicide attack in 1981, although some prior attacks could be considered suicidal. It records 37 suicide attacks between 1981 and 1990 and 150 in the following decade (1991–2000). The total ascended to 1,706 in the years between 2001 and 2010, and for the five years from 2011 to 2015, the GTD records a total of 2,878 suicide attacks.[9]

However, the distribution of these attacks underscores the point made earlier that terrorism is a specific component of contemporary warfare. Of the 2,878 suicide terrorist attacks that took place between 2011 and 2015, 2,402 (or 83 percent of them) occurred in just six countries: Iraq (1,034), Afghanistan (682), Pakistan (217), Syria (203), Nigeria (203), and Yemen (63). Suicide attacks have become a routine tactic of primarily, but not exclusively, jihadist warfare.[10]

The MTI database shows a similar increase in suicide attacks on surface-transportation targets. The first recorded suicide attack on surface transportation occurred in 1993. For the decade between 1991 and 2000, there were 22 such attacks; between 2001 and 2010, there were 82; and there were 65 between 2011 and 2015. The much lower totals than those in the GTD again reflect MTI's deliberate exclusion of war zones and the fact that MTI's database encompasses a much narrower target set.[11]

Suicide attacks comprise only a tiny portion of the total attacks on surface transportation. However, if the 1,919 total attacks between 2011 and 2015 in Afghanistan, Iraq, and Syria are excluded from the GTD data, leaving 959 suicide attacks in the countries included in the MTI database, then the 124 suicide attacks on

Approximately one out of every eight suicide bombings has targeted public surface transportation.

surface transportation represent 13 percent of the total number of suicide attacks against all targets. In other words, approximately one out of every eight suicide bombings has targeted public surface transportation. Caution is in order here, as the GTD data need to be more closely examined before a valid comparison can be made, but this finding does suggest a worrisome trend.

TERRORIST GROUPS ARE OPERATING MORE GLOBALLY

Analysts in the 1970s tried to anticipate the next terrorist weapon. Would terrorists use precision-guided weapons, remotely piloted vehicles, chemical or biological agents, possibly even nuclear weapons? The analysts, including me, failed to recognize, however, that terrorism is about communications, not battle. They did not include the Internet, which hardly existed then but which eventually enabled terrorist organizations to publicize their propaganda with little interference by censors or editors, to communicate with supporters and potential recruits worldwide, and to inspire and exhort others to carry out attacks in distant locations, thus enabling them to bypass border controls. While warfare declined in general, wars were more likely to include terrorist attacks that could occur anywhere in the world.

In summary, then, terrorism in its current form emerged in the late 1960s, and by the mid-1970s, terrorists had established their tactical repertoire. It has changed only incrementally since. The volume of terrorist attacks has increased dramatically since 1970, although much of this increase reflects better reporting and the fact that terrorism has become an increasingly routine component of warfare. Terrorists have also escalated their violence. Achieving the goal of large-scale casualties requires less-discriminate attacks, but changing terrorist motives and norms made this less of a problem for the terrorists. The adoption of suicide attacks on a wide scale has resulted in higher levels of lethality and has further added to public alarm. And terrorists are effectively exploiting the Internet to explain their cause, reach broader audiences, attract recruits, and create global networks.

III. HOW TERRORISM DIFFERS FROM CERTAIN FORMS OF CRIME AND OTHER MODES OF ARMED CONFLICT, AND THE IMPLICATIONS FOR SECURITY

Terrorism poses novel problems for security planners. Terrorist attacks differ from more-conventional modes of armed conflict and from other categories of violent crime. Unlike military units, terrorists do not have to attack certain targets in a specific time frame to achieve results. And unlike criminals who engage in armed robberies or burglaries, terrorists do not have to risk exposure by penetrating guarded facilities to get at some desired treasure. That gives terrorist attackers an inherent advantage. They can attack anything, anywhere, any time, while authorities cannot protect everything, everywhere, all the time.

Terrorists do not organize into armies. They operate clandestinely, and they offer few clues about where they might attack next—despite intense intelligence efforts, surprises must be assumed. And the availability of virtually unlimited targets for terrorist attacks makes it difficult to decide where and how limited security resources should be allocated to protect the targets that terrorists might strike. Traditional threat assessments are based on analysis of the adversary's intentions and capabilities, but these count less in predicting what terrorists might attack. Unconstrained in their choice of targets, terrorists can select any target within the range of their capabilities.

The availability of virtually unlimited targets for terrorist attacks makes it difficult to decide where and how limited security resources should be allocated.

Security planners have therefore been pushed toward vulnerability-based analyses. Instead of starting with what is known about the threat, vulnerability-based threat assessment starts by identifying potential targets—something that terrorists might attack, then positing a hypothetical terrorist foe, and outlining an invariably worst-case scenario. Vulnerability-based analyses are useful in looking at the potential consequences of potential attacks and evaluating preparedness. They are not threat assessments, but they tend to be treated as if they described actual threats.

A further problem with vulnerability-based analysis begins with the word *vulnerability* itself. It concentrates the mind on the dire things that could happen—it is a victim's perspective. The 9/11 attacks demonstrated America's vulnerabilities. These attacks produced less death and destruction than was envisioned in Cold War imaginings of a nuclear attack, but 9/11 may have had greater visual impact because instead of the instant vaporization and incineration that comes with a nuclear explosion, the slow-motion collapse of the Twin Towers was observable and was watched by millions of people hundreds of times. Terrorist threats could be reduced and security could be increased, but the indelible sense of vulnerability created on 9/11 was recalled again and again in subsequent discussions of possible terrorist scenarios.

Different terrorism scenarios compete for limited security resources. Advocates who are worried about a particular terrorist weapon or potential target set argue that the

consequences of their particular scenario are worse than those of the other competing scenarios and hence deserve more attention and funding. In this debate, the catastrophic consequences of worst-case scenarios outweigh their probability of occurrence. The competition for security resources also involves bureaucrats who want to avoid any future culpability by being seen protecting their areas of responsibility.

In a democracy, much of such discussion takes place in the public domain. The discussion itself inspires terrorists to think about whether they are actually capable of carrying out the imagined scenarios. Even if they are not, talking about these scenarios fulfills terrorist fantasies while we listen. Eavesdropping authorities may then interpret the terrorists' discussions as confirmation of assumed intentions, thereby confirming their worst fears. The endless public discussion of dire terrorist schemes also contributes to public alarm. When Americans ask whether we are safer now, they are not seeking an objective measure, they want the feeling of vulnerability to go away. The continuing discussion of vulnerabilities ensures that it will not.

When Americans ask whether we are safer now, they are not seeking an objective measure, they want the feeling of vulnerability to go away.

TERRORISTS ATTACK SOFT TARGETS

Another unique attribute of terrorism is its focus on soft targets. By definition, terrorist attacks are aimed at targets that ordinarily would not be attacked, according to the rules of war. However, within this category, some targets are better protected than others. Terrorists can obviate physical security measures by attacking unprotected targets—that is, they can attack unprotected civilians, and they can carry out armed assaults or plant bombs in locations where there is little or no surveillance, no security perimeters to penetrate, and few, if any, armed guards to respond. Recent terrorist targets have included churches, synagogues, mosques, schools, restaurants, theaters, markets, shops, apartment buildings, private homes, and public gatherings—some of which now have increased security, as a result of the terrorist attacks. Targets such as train tracks and pipelines can be bombed without risking encounters with security forces. Bombs and land mines can be planted on roads and detonated automatically or remotely.

Terrorists also can obviate security measures by employing tactics such as drive-by shootings, by tossing explosive or incendiary devices from cars, or by standoff attacks—firing mortars or rockets at distant targets. Terrorists can set off bombs in the general vicinity of their target, leaving it to the media to make the connection. For example, detonating a bomb in the vicinity of an embassy or other government building or outside a corporate headquarters avoids security and incurs little risk to the bombers but achieves almost the same coverage as a bomb at the target itself.

It is sometimes difficult to make judgments about how to categorize certain attacks on what appear to be harder targets—for example, when attackers approach security checkpoints and then open fire or detonate bombs. Such attackers recognize that security measures are in place or nearby and therefore know that they may be apprehended or killed in the encounter, but they still hope to cause casualties before they are neutralized. Security may

prevent the attackers from getting to the actual target, but an attack still takes place, and the attempt itself is often portrayed as a terrorist success.

A sample of 200 terrorist attacks recorded in the GTD gives us a rough idea of how often terrorists avoid security measures. One hundred incidents were selected at random from the period 1970–1979, and another hundred were selected at random from 2000–2009.[12] The incidents were sorted by target category and terrorist tactic.

In the 1970–1979 period, terrorists in the sample attacked 84 unprotected targets—targets where there were no security perimeters and no guards. The targets included a theater, a restaurant, a union headquarters, a primary school, a university campus building, a synagogue, a post office, a bank, a bus station, and several corporate headquarters. Seven of the attacks would have required penetration of a target that was likely to have some form of security perimeter, not necessarily a daunting one, or would have exposed the attackers to a response by armed security personnel. Nine attacks had to be categorized as "unknown," owing to a lack of information about security measures that may or may not have been in place.

The results were similar for the randomly selected incidents in the 2000–2009 period: 75 of the attacks involved unprotected targets, including churches, mosques, a synagogue, several schools, open-air markets, a bakery, a real-estate office, mobile-phone shops, buses, tourists, railroad tracks, a pipeline, "near a hotel," and "in the vicinity" of an embassy. Seventeen attacks involved some level of security, and eight fell into the unknown category.[13] The higher number of attacks in which terrorists had to deal with security reflects increased reporting from war zones such as Afghanistan and Iraq, where terrorists often blew themselves up at security checkpoints. Whether attacks on military personnel or other security-force targets should be included in the definition of terrorism, even if they take the form of roadside or suicide bombings, is another issue.

Although these numbers derive from a random sample and some of the events call for judgment, the overall pattern seems clear. In approximately 80 percent of the incidents, security measures were irrelevant because the terrorists attacked unprotected targets. Another observer might categorize a few of the incidents differently, but this would not be likely to change the overall conclusion. Security did not *fail*—it simply was not there. Nor is this to say that security is completely irrelevant to terrorism; it still affects terrorist decisions about what to attack or the tactics to employ. The fact that terrorists concentrated their attacks on unprotected targets, however, suggests that they avoided protected targets, and that in itself can be seen as evidence that security works.

In approximately 80 percent of the incidents, security measures were irrelevant because the terrorists attacked unprotected targets.

There are exceptions to the preference for soft targets. Some terrorists appear to remain obsessed with attacking certain target sets despite the increasing difficulties of doing so. Commercial aviation is one example. Although increased security measures have made it more difficult to smuggle weapons or bombs aboard airliners, terrorists continue to try to develop ways of getting past these measures. Wile terrorist hijackings have declined overall, as have sabotage attempts, some terrorists continue to try to smuggle bombs aboard

airliners either by building smaller, more easily concealed devices that can avoid detection or by utilizing inside accomplices. And even as attacks on airliners have declined, aviation remains in their sights, as terrorists have attacked airports and even airline ticket offices.

Faced with the "ring of steel," an array of security measures put into place after the first major terrorist bombing in London's financial district, the Irish Republican Army (IRA) built a huge truck bomb and patiently waited months for an opportunity to strike again. When security was altered to facilitate the passage of construction vehicles engaged in the project to repair the damage of the first bombing, the IRA promptly exploited the opening and struck a second time.

Following a terrorist car bombing of a Marriott hotel in Jakarta, security at the property was significantly increased. The terrorists then prepared another large bomb, which they could have used against other hotels in Jakarta that had far less security. Instead, they employed an insider to set off two small bombs inside the lobbies of the JW Marriott hotel and the adjoining Ritz-Carlton hotel. Although easier target venues were available, and reportedly had a vehicle bomb ready to be used in an attack, the terrorists wanted to demonstrate they could overcome even the most stringent security measures. In their view, the prestige that the demonstration of determination and prowess would bring them was worth the added operational risk.[14]

TERRORIST ATTACKS ARE STATISTICALLY RARE AND RANDOM

While the volume of terrorism in the world has increased significantly and thousands of terrorist incidents now occur worldwide every year, causing casualties and property damage, terrorism still represents only a tiny fraction of the collective and individual violence in the world. Terrorist attacks remain statistically rare and random, especially outside of conflict zones. This is particularly true in the United States, where since 9/11, terrorists motivated by jihadist ideologies—the source of the principal terrorist threat over the past 15 years (although many people would argue that white supremacists and anti-federal government extremists also pose a significant threat)—have killed fewer than 100 persons, an average of six deaths a year. While every such death is a needless tragedy, this is a much better result than most people feared or expected immediately after 9/11, and deaths from terrorist attacks represent only a tiny fraction of the approximately 15,000 homicides that occur annually in the United States.

That makes it hard to determine the right level of security. With risks to individual citizens and specific target sets so low, almost any expenditure on security against terrorism may appear extravagant. Critics of security are fond of pointing out that bee stings and spider bites pose a greater threat to Americans than terrorists do.[15] This ignores the psychological consequences of terrorism, but the low level of violence also makes it nearly impossible to measure the amount of reduction in risk security brings—it cannot be significant because the totals are so low to begin with. Critics can easily lambaste security against terrorism as not worth the money, and certainly not worth the disruption and imposition on individual liberty.

With risks to individual citizens and specific target sets so low, almost any expenditure on security against terrorism may appear extravagant.

Including the 9/11 attacks, however, alters the calculation. Most people would agree that security should be in place to prevent another 9/11. But that is a single scenario—one that government officials stand accused of having failed to envision—and it would seem dangerous not to consider and protect against other scenarios of similar magnitude. That, however, puts security planning into the realm of imagination, where what drives security is not what terrorists have done, but rather, what terrorists conceivably might do in the future. In that realm, where are the boundaries?

Security planners must deal with considerable uncertainty in assessing the terrorist threat and in calculating the appropriate response. What is the level of risk? How much security is enough? How far should security planners go in dealing with terrorist scenarios that are theoretically plausible but have not yet occurred?

Terrorists, along with analysts trying to think as terrorists, can conjure up more scenarios of mayhem and mass destruction than those charged with security can take measures to protect against. The attacks on 9/11 fundamentally altered perceptions of plausibility. Scenarios that had been previously dismissed as far-fetched became operative presumptions the day after those attacks.

Should the threshold for taking new security measures be that terrorists have already demonstrated their intentions and capabilities to carry out such attacks, perhaps more than once? If that is the case, security planners might risk another failure of imagination. And does it make a difference where and under what circumstances the precedents took place? For example, large-scale suicide attacks in a conflict zone like Afghanistan or Syria may not indicate that such attacks are just as likely in America or Europe, but, as we have seen in the United Kingdom, France, and Belgium and in terrorist plots in the United States, neither are they impossible.

And preparing only for what has already happened makes security reactive. Many would argue that such a posture guarantees future security failures. Should the threshold instead be lowered to what we know terrorists have contemplated but not yet done? We know that many of the attacks terrorists have thought about are ambitious fantasies. Should terrorist scenarios be taken seriously by security planners if there is even a 1-percent chance of an actual attempt? (This was the so-called Cheney Doctrine.)

Many of the attacks terrorists have thought about are ambitious fantasies.

Or should defenses be based upon what pundits can imagine? There is no agreement on how much attention and resources should be devoted to less-likely threats, but the pressure is on security to address everything, no matter what the odds, especially when the consequences are severe.

Devoting vast resources to events of uncertain probability but with potentially catastrophic consequences is not unique to terrorism. The United States spent vast sums on maintaining a huge nuclear arsenal during the Cold War because the threat of nuclear war was viewed as existential. Lesser wars were tolerable. In the case of terrorism, however, tolerance for failure is much lower. The fact that *any* terrorist attacks have occurred in the U.S. homeland

causes apprehension and outrage and further complicates security calculations. That is due to the nature of terrorism itself.

TERRORISM IS, ABOVE ALL, PSYCHOLOGICAL WARFARE

Terrorism is defined as violence—actual or threatened—calculated to create fear and alarm, i.e., terror. Terrorism is aimed at the people watching. Its effects are, above all, psychological. The creation of terror causes people to exaggerate the importance of the terrorists and the threat they pose. Terrorism, therefore, is much more a matter of perceptions than of easily quantifiable risks or losses.

Terrorism...is much more a matter of perceptions than of easily quantifiable risks or losses.

This observation has profound implications for security. To be successful in creating terror, terrorists do not have to directly defeat security measures. They rely not on their ability to defeat security, but on their ability to create terror. Terrorism—the actions of terrorists—and terror—the psychological effects of terrorist actions—are separate domains. Even low levels of terrorism can (and do) produce high levels of alarm. Therefore, terrorists with limited capabilities and minimal resources can achieve major effects.

This is especially true in the context of today's media-drenched society. Media coverage, particularly visual media coverage, greatly extends the reach and effects of terrorism. If terrorism is theater, contemporary communications, through mass and social media, enable terrorists to reach an audience of global proportions almost instantaneously. The mass media also tend to increase the drama by repeatedly broadcasting the visuals that terrorists choreograph, by endless speculation about what could occur, and by mobilizing legions of talking heads to further discuss the matter—and in the discussions, those making the most dramatic claims, those describing worst-case scenarios, have an advantage over those counseling calm.

Partisan politics further incentivize the creation of fear. Every terrorist incident is portrayed as a failure for which someone is to blame and heads must roll. Politicians pound podiums and point fingers. They demand that more be done to protect people. It is politically safer to support increases in security than to oppose them. Even those who see little utility in proposed measures risk condemnation for substandard zeal, for imperiling the lives of citizens if they do not agree and being pilloried if another attack occurs—any terrorist attack, which most likely will happen. And if security is therefore to be increased despite the uncertainty, it must be argued that the threat warrants an increase. In other words, fear drives security decisions that, once made, must be supported by a commensurate level of assumed threat, so security also drives threat portrayals. There is no point in diminishing the dragons one promises to slay.

Every terrorist incident is portrayed as a failure for which someone is to blame and heads must roll.

By demanding and unrealistically expecting absolute security, the public contributes to its own fear. It encourages the government to overpromise what it can deliver, setting it up for failure, which will, in turn, exacerbate public alarm. Terrorism theoretically could

be attacked by reducing terror, that is, by fostering a psychologically less-vulnerable society, thereby reducing the ability of terrorists to create fear. However, appeals to courage, stoicism, and self-reliance, although these are considered traditional American attributes, have not been a major feature of U.S. counterterrorism strategy.

Appeals to courage, stoicism, and self-reliance, although these are considered traditional American attributes, have not been a major feature of U.S. counterterrorism strategy.

Terrorists do not have to succeed tactically to get media attention and create alarm. A terrorist bomb may fail to kill anyone—it may not even work—but its mere discovery can cause fear that there may be other undiscovered devices or that a determined person or group may succeed the next time. At a minimum, an attempted terrorist event will be viewed as a failure of security, which must then be increased to prevent further such events.

There are numerous examples. In 2001, a terrorist attempted to detonate a bomb concealed in his shoe while aboard a U.S.-bound flight. The device failed to go off, and the bomber was quickly subdued, but the fact that security measures had failed to prevent him from boarding the flight resulted in the implementation of new screening measures at airports. In the United States, it led to the requirement for passengers to remove their shoes and place them on the conveyer, where they could be x-rayed.

In 2006, British authorities uncovered a plot to smuggle liquid explosives on board airliners flying out of Heathrow Airport. The plot was foiled, but it nonetheless caused great concern and promptly led to restrictions on the amount of liquids passengers could carry.

In 2009, one of al Qaeda's regional affiliates sent a Nigerian recruit with a small bomb concealed in his underpants to destroy an airliner flying from Amsterdam to Detroit. The terrorist managed to get on board with the device, but when he tried to ignite it, it did not work, and passengers quickly immobilized him. Despite the failure, the U.S. government responded by deploying body scanners at a cost of hundreds of millions of dollars and implementing new, more-thorough pat-down procedures.

Although they failed to bring down any airliners, the terrorists in all three of these cases achieved enormous psychological and economic effects, proving that results can be achieved independent of the actual loss of life or physical destruction, based solely upon perceptions of risk, which are distorted by fear and alarm and often exacerbated by public reactions and partisan politics. These examples also show that each new demonstrated terrorist capability requires an enormous financial outlay to counter the threat.

The jihadists clearly have discovered this and have recently modified their strategy to exploit these vulnerabilities. Jihadist rhetoric now urges followers to launch attacks, even if they are likely to fail, confident that public and political reactions will still provide a good return on their investment.

Jihadist rhetoric now urges followers to launch attacks, even if they are likely to fail, confident that public and political reactions will still provide a good return on their investment.

All of this suggests that security measures should not consist solely of physical measures but should also address social consequences. For example, authorities might think more about how to create a more resilient society and a political environment that discourages rather than encourages overreaction.

This section has attempted to show that terrorists have significant advantages over security planners. Terrorist targets are unlimited, while it is impossible to protect everything. Terrorists obviate security measures by attacking soft, unprotected targets—indeed, most terrorist attacks are aimed at such targets. And while terrorism has increased in volume, it remains statistically rare and random, complicating calculations about the right level of security. On one hand, the risk to the individual citizen seems too low to justify massive security measures. On the other hand, authorities must anticipate and try to prevent low-probability events that have potentially severe consequences. Public fear further distorts the process. Terrorists aim at gaining attention, causing alarm, and creating the apparent necessity of increasing disruptive and costly security measures, and they can succeed in doing so with low level attacks and even with foiled plots and failures.

IV. THE CHALLENGE OF TERRORISM FOR SECURITY

WHAT IS SECURITY SUPPOSED TO ACHIEVE?

Security against terrorism can be broadly defined to include everything a country does to protect its national interests and citizens against terrorist attacks abroad and at home—foreign and domestic intelligence efforts, diplomacy, direct military operations and military assistance to allies, international and domestic law enforcement efforts, visitor and border controls, physical protection measures, and effective response to attacks that occur. Security is not just what government does, it also includes all of the security measures taken by the private sector to protect critical infrastructure, facilities, and people. While this report addresses only one aspect of security—the physical security measures in place to prevent successful terrorist attacks against specific targets—it is important to keep in mind that these measures are only one component of a broader national effort. Security can be intended to achieve a variety of goals, including those described below.

Eliminate terrorist groups. Security against terrorism in the United States is a component of the federal government's responsibility, as written in the U.S. Constitution, *to provide for the common defense*. However, there is a difference between providing for the national defense and protecting every citizen against attack. Terrorists make no distinction between front lines and home fronts, between combatants and noncombatants. Defending the nation does not mean guaranteeing no domestic casualties.

There is a difference between providing for the national defense and protecting every citizen against attack.

The government's active counterterrorism efforts are aimed at eliminating the terrorist groups that pose a threat to the nation's security. But if it were possible to destroy all of the groups that might threaten the United States before they could mount any attack, there would be little need for security in any other form. Eliminating terrorist groups, like combating crime, however, is a difficult and enduring task. Victory in the traditional military sense may not be achievable.

Deter terrorists from attempting attacks. Security measures can succeed by deterring adversaries from attempting to carry out attacks. In the Cold War, the risk of retaliation discouraged the Soviet Union (and the United States) from using nuclear weapons. Deterring terrorists works differently. Retaliation may have a deterrent effect in some cases, but deterrence against terrorist attacks through protective measures alone requires deploying levels of security that come close to guaranteeing operational failure by any attacker. Passenger screening at airports is an example. Security at this level requires significant resources, causes inconvenience, and even then does not guarantee absolute prevention.

Uncover and thwart terrorist plots. Intelligence efforts to uncover and thwart terrorist plots play a major role in counterterrorism security. U.S. authorities have had remarkable success in interrupting terrorist plots. It is likely that not all of the plots uncovered would have resulted in attacks had they not been discovered, but some would have. The ability of the authorities to penetrate terrorist conspiracies and bring would-be terrorists to justice may also contribute to a deterrent effect.

At the same time, domestic intelligence efforts, while effective, are controversial. In some cases, they are seen to pose threats to individual liberties. Perceptions of necessity and public tolerance depend on levels of fear, which are highly subjective. In a democracy, this will always be a source of tension—I would add, as it should be.

Prevent successful attacks. When deterrence and intelligence have failed, physical security measures are the last line of defense. They aim at detecting and promptly neutralizing any attack before the terrorists can reach their intended target and carry out their mission. This is important to remember when evaluating these measures. In most cases, they come into play as a response to a terrorist operation that has begun. In other words, the attackers are there, driving toward their target, climbing over the fence, coming through the door, or at a security checkpoint, with weapons or explosives. The news media and some critics portray even attempted terrorist attacks, whether or not the attackers succeed, as security failures. In the broadest sense, these events *are* failures of some aspect of security, but not necessarily because the security measures surrounding the target failed.

Reduce the consequences of terrorist attacks. Measures to mitigate casualties, damage, and disruption should be included in a broad definition of security. Aviation security is front-loaded—it invests heavily in prevention. Failure to prevent attacks on airliners allows little mitigation. When a plane is taken over by hijackers, hundreds will be in peril and may be killed. Prevention of attacks on public surface transportation is more difficult. The volumes of passengers, requirements for access, need for speed, and cost considerations limit what realistically can be done to keep terrorists away from the target. Surface-transportation security is more heavily back-loaded, comprising measures such as design and construction features aimed at mitigating the effects of explosions, facilitating easy surveillance and rapid response, making evacuation easier, and rapidly restoring service to minimize disruption. Much more emphasis in recent years is being placed on resilience, which is itself a recognition of the limits of prevention.

Prevention of attacks on public surface transportation is more difficult. The volumes of passengers, requirements for access, need for speed, and cost considerations limit what realistically can be done.

The focus in this report is on security more narrowly defined, that is, the physical and procedural measures in place to prevent successful terrorist attacks against specific targets. Again, the emphasis is on empirical evidence of the effects and effectiveness of these measures.

HOW MUCH DOES THE UNITED STATES SPEND ON SECURITY AGAINST TERRORISM?

It is difficult to calculate exactly how much is spent in the United States on security against terrorism. If the total costs of U.S. military operations in Afghanistan, Iraq, and elsewhere are included in a counterterrorist budget, the figure ascends to the trillions of dollars. That is not what we are looking at. What we want to know is how much federal, state, and local

governments and the private sector spend on domestic security measures against terrorism. The difficulties here are in compiling total expenditures and in trying to separate the incremental costs of security against terrorism from the costs of security against ordinary crime and other threats.

What we want to know is how much federal, state, and local governments and the private sector spend on domestic security measures against terrorism.

Federal expenditures to provide security against terrorism are not simply synonymous with the budget of the Department of Homeland Security. That budget covers activities that would continue if there were no terrorist threat—customs and border patrol, presidential protection, response to natural disasters, etc. At the same time, other federal agencies also spend money on protection against terrorism. A total budget for security against terrorism would include these incremental expenditures of all federal agencies.

An analysis of such expenditures, mandated by Congress, concluded that not counting the costs of intelligence or military operations, the federal government spent a little over $72 billion on homeland security specifically aimed at terrorism in fiscal year 2015.[16] The analysis breaks the expenditures down into three broad categories: programs to disrupt and prevent terrorist attacks ($35 billion); programs to protect the American people, critical infrastructure, and key resources ($26 billion); and programs in place to respond to and recover from incidents ($11 billion). Excluding recovery costs, the $61 billion for the first two programs would approximate the federal budget for *security* against terrorism.[17]

It is more difficult to calculate how much state and local governments are spending to secure their jurisdictions specifically against terrorism. A study by RAND researchers published in 2008 estimated those state expenditures at $1 billion to $2 billion a year (not counting federal grants) and private sector expenditures at $5 billion plus another $5 billion in added insurance costs.[18] A 2011 study estimated that spending for security against terrorism by state and local governments and the private sector totaled $100 billion for the decade after 9/11, or approximately $10 billion a year.[19] (It is not clear whether this figure includes incremental insurance costs.) Adding state and local expenditures to the federal government expenditures results in a total estimate of somewhere between $67 billion and $71 billion a year. Is security against terrorist attacks, which can never prevent all attacks, worth it?

Adding state and local expenditures to the federal government expenditures results in a total estimate of somewhere between $67 billion and $71 billion a year.

At a glance, this would seem to be an easy question to answer. The country has invested heavily in homeland security and is safer now. In fact, in terms of terrorist activity in the United States, the years since the 9/11 attacks have been the most tranquil since the 1960s, when terrorism in its contemporary form first emerged as a threat. Whether Americans think they are safer from terrorism is a different question.

Most Americans tend not to recall that during the 1970s, the United States experienced an average of 50 to 60 bombings a year. These were carried out by a variety of mostly terrorist

groups (leftwing extremists like the Weather Underground and New World Liberation Front, white and black supremacist groups, Puerto Rican separatists, anti-Castro Cuban extremist groups, Palestinian terrorist organizations, the Jewish Defense League, Croatian separatists, and others).

In the more than 15 years since the 9/11 attacks, terrorists inspired by al Qaeda's ideology of violent jihad or that of the Islamic State of Iraq and the Levant (ISIL) have carried out 16 attacks in the United States. Seven of these cases resulted in fatalities.[20] Six attacks were by lone gunmen and resulted in 70 fatalities. In two of the attacks, two shooters were involved. These include the 2015 shooting in Garland, Texas, in which only the assailants were killed, and the shooting in San Bernardino, which resulted in 14 deaths, not counting the assailants who were later killed in a shootout with police. Three attacks involved attempted bombings. One of these, the bombing in Boston in 2013, killed three people (during their escape, the bombers also killed a policeman, the fourth fatality, and wounded another policeman who died months later as a consequence of his injuries, which counts as a fifth fatality in the case), bringing the total of fatalities in this period to 89. Three attacks involved stabbings or an assault with a hatchet, and two involved ramming cars into pedestrians.[21] Attacks categorized as hate crimes but not terrorism—a blurry boundary separates the two—would add a few more to the total.

Several of the events categorized as acts of terrorism are controversial. Some would argue that Nidal Hasan's killing of 13 people at Fort Hood, TX, should not be categorized as an act of terrorism, but rather as the violent acting out of a disturbed individual, even though there is evidence of his correspondence with a known al Qaeda leader. The federal government considered that attack to be an act of workplace violence, which it certainly was, but it can also be seen as a politically motivated attack. (I would put it in the terrorism column.) The attacker in an incident in Chattanooga, TN, had a history of mental problems and substance abuse. A mentally disturbed individual who has looked at a terrorist website or claimed allegiance to a distant group cannot automatically be labeled a terrorist. Adding or subtracting a handful of cases, however, does not change the fact that these are very small numbers.

CAN COST-BENEFIT ANALYSIS BE APPLIED TO SECURITY AGAINST TERRORISM?

Have the visible security measures that are so prevalent in the landscape prevented more terrorist attacks? Intelligence operations clearly have been successful. Federal investigators and local police have uncovered and thwarted more than 80 percent of the jihadist terrorist plots in the United States. This is not to claim that every interrupted plot would have resulted in an attack had authorities not intervened, but some certainly would have. Whether the physical measures in place have reduced the risk of terrorist attack is more difficult to determine. The empirical evidence is slender.

Critics of the current security regime argue that the terrorist threat to the United States is overblown. In their view, the risks involved are simply too low to justify the massive outlays in security. Cost-benefit analysis, these critics argue, shows that "in order to be deemed cost-effective [these measures] … would have to deter, prevent, foil, or protect

against 1,667 otherwise successful Times-Square-type attacks per year, or more than four per day."[22] (The Times Square attack refers to the attempted bombing of New York's Times Square by Faisal Shahzad in 2010 in which Shazad's device failed to detonate and no one was killed.)

Critics of the current security regime argue that the terrorist threat to the United States is overblown.

The 9/11 attacks have thus far proved to be a statistical outlier, not an indicator of many more large-scale attacks to come, yet government officials continue to focus on worst-case scenarios and neglect probabilities. However, officials focus on worst-case scenarios, not because they overestimate the likelihood of such scenarios, which, in fact, is unknowable, but because the potential catastrophic consequences assumed in the worst cases overwhelm all other variables. And consequences are almost invariably calculated on the basis of worst-case scenarios. In some analyses, consequences are deliberately weighted to count more than threat. The result is that the consequences of an event overwhelm the probability of its occurrence, particularly when that probability is very remote. Essentially, risk calculations are consequence-driven.

Officials also focus on higher-register events as the appropriate realm of federal government activity. Government officials are not convinced that they can prevent the lower-level attacks carried out by individuals or tiny conspiracies, but failure to stop every low-level attack will not bring down the republic, while failure to stop an attack on the scale of 9/11 could have devastating psychological, economic, and political consequences for the nation.

Government officials, however, operate under enormous public and political pressure to prevent all attacks. They are hardly allowed to manage risk; expectations are too high. Again, defense of the nation—a government's primary duty—does not mean guaranteeing the security of every individual. In this regard, the public's expectations are unrealistic, and the government is pushed to overpromise security.

Government officials...operate under enormous public and political pressure to prevent all attacks.

Cost-benefit analysis also fails to fully appreciate the role of terror. Casualties cannot be the sole currency of exchange. Deaths from terrorist attacks have far greater psychological effect than those resulting from other forms of violent crime that have, unfortunately, become common occurrences. Homicides in the United States currently number about 15,000 a year, down from 24,000–25,000 a year in the early 1990s. This decline would allow three attacks a year on the scale of 9/11 without raising the overall risk of violent death at the hands of an individual. But one 9/11-scale event a year probably would imperil America's democracy. Overreaction, fueled by intense and often lurid media coverage and political partisanship, also guarantees that even smaller-scale events will achieve disproportionate effects.

Cost-benefit analysis is useful in forcing officials to articulate their presumptions and make explicit tradeoffs. In my view, while accepting that resources are not unlimited and

therefore choices have to include cost considerations, cost-benefit analysis cannot be dispositive in determining security measures—almost none would be considered worth it. These comments will no doubt provoke a vigorous response.

Cost-benefit analysis cannot be dispositive in determining security measures—almost none would be considered worth it.

SECURITY ENCOMPASSES A CATALOG OF MEASURES

Security comprises a broad array of laws, technology, and procedures calculated to reduce terrorist capabilities, detect potential terrorist attacks, impede terrorist operations, and facilitate prompt response. The basic concepts of security have not changed since the Middle Ages, but the continuing challenge of crime and the new challenge of terrorism have produced some dramatic changes in responses since 1970. Closed-circuit television (CCTV) surveillance systems have become ubiquitous in public areas, especially in the United Kingdom and the United States. These are now backed up by sophisticated computerized analytics that can detect aberrations from normal patterns of activity and signal alarms.

The threat of terrorist kidnappings spawned a personal protection industry that provided armored cars, chauffeurs trained in defensive driving, armed bodyguards, kidnap and ransom insurance policies, and hostage recovery consultants.

Bombings, the most frequent terrorist tactic, have pushed the development and deployment of explosives-detection systems. Bombings also have encouraged the proliferation of inner perimeters protected by access control systems. Imaging systems capable of detecting concealed weapons or explosives have been greatly improved. Advances are being made in remote detection. Terrorist use of large, vehicle-borne explosives has led to the widespread erection of physical barriers and the development of blast-resistant materials for construction and glazing. Embassies are now built for defense.

Advances in information technology have enabled data from multiple sources to be aggregated and analyzed to detect suspicious activity and track suspects. The growing capacity of information systems to monitor, collect, store, retrieve, and mechanically analyze vast amounts of data about individual citizens and use those data to detect suspicious individuals and behavior is controversial. Behavioral detection is a more recent and even more controversial addition to security measures. Current behavioral-detection efforts depend on individual training, but new systems based solely on technology are under development.

Current behavioral-detection efforts depend on individual training, but new systems based solely on technology are under development.

Recent decades have also seen institutional developments. Intelligence efforts have been refocused and expanded enormously, especially in the United States since 9/11 and increasingly in Europe in the wake of recent terrorist attacks, despite much stricter privacy laws. New laws have been passed to facilitate intelligence collection and broaden police powers. In some countries, periods of preventive detention have been lengthened and new administrative controls like house arrest have been imposed. In an effort to reduce

radicalization and recruitment to terrorist ranks, controls have been imposed on speech and Internet communications. What the law considers to be incitement has been expanded. Efforts to better understand and counter violent extremism are being increased.

While much of security remains a private sector responsibility, the continuing terrorist threat has led governments to play a larger role in disseminating best security practices, mandating minimum security requirements, and, in some cases, directly implementing security measures—as, for example, in airline passenger screening in the United States. In response to the threat that terrorists may attack anywhere, members of the public have been mobilized to bring suspicious behavior or objects to the attention of the authorities. This measure is discussed later.

Although these measures do not in themselves "catch" terrorists, each contributes directly and indirectly to security. A brief description of counterterrorism security measures and how they came about and are intended to work is given below.

Intelligence. Although intelligence efforts are separate from the physical security measures discussed here, they warrant mention. Following 9/11, the United States devoted an enormous effort to improving its foreign and domestic intelligence capabilities. Information-sharing and coordination were increased. The U.S. effort was assisted by unprecedented cooperation among intelligence services and law enforcement organizations worldwide. While still not optimal, domestic intelligence has also greatly improved and has achieved a remarkable record in preventing terrorist attacks, although some of the investigations and prosecutions have caused concern from the perspective of civil liberties.[23] Intelligence is the first line of defense and has become the most effective component of the overall security effort.

Watch lists. Watch lists are used to identify potential terrorists and deny them access; the lists have grown dramatically since 9/11. Connecting and consolidating the various lists and making them instantly accessible to appropriate users has been a major achievement. The U.S. government's central database of known or suspected international terrorists (which may include U.S. citizens operating under direction from abroad), the Terrorist Identities Datamart Environment (TIDE), reportedly includes more than a million names. The FBI maintains a smaller list of suspects in its Terrorist Screening Database, which, in turn, is used to compile specific lists such as the no-fly list. These watch lists now guide security efforts, although they remain controversial.

Computer-Assisted Passenger Pre-Screening System (CAPPS). Watch lists are intelligence-based. CAPPS is behavior-based. CAPPS was introduced to aviation security in the 1990s, following the recommendation of the White House Commission on Aviation Safety and Security. CAPPS analyzes the information available in the Passenger Name Record (PNR) that is created when a traveler books a flight, according to an algorithm that ranks the passenger according to potential risk. It is a mathematical application of the approach initially developed by Israel's El Al Airlines for passenger pre-screening, which was based on a review of passenger information and sometimes intensive interviews with passengers prior to boarding. (El Al had the advantage of comparatively few flights and a unique passenger composition that made it easy to determine that the bulk of its passengers posed little or no risk.)

Larger passenger loads (currently an average of more than two million airline boardings a day in the United State), a more diverse passenger composition, and greater sensitivity to what appears to be any sort of profiling—in violation of civil liberties—made the Israeli model inapplicable in the United States. A less-subjective, mathematically based screening system was considered more acceptable, especially when the system was designed to randomly add passengers, thereby guaranteeing that passengers selected for additional scrutiny would not be treated as suspects; it also made the system more difficult for potential adversaries to game.

The airline industry opposed the introduction of CAPPS on grounds that it initially required selected passengers to be taken directly to security, where they would be subjected to additional screening, slowing down the screening process overall. Its implementation was modified to make a selection by CAPPS relevant only for the passengers' checked baggage. A selectee's baggage had to be inspected. Therefore, when CAPPS identified more than half of the hijackers on the morning of September 11, 2001, it had no effect on their screening. An improved system called CAPPS II was proposed by the U.S. Transportation Security Administration (TSA) in 2003 but was opposed by civil libertarians and blocked by Congress. The initiative was terminated by President George W. Bush in August 2004.

Although some airlines still use CAPPS or variations of the systme and pass the information on to TSA, the United States has moved away from CAPPS toward what is believed to be a more efficient method of assessing passenger risk by adopting Pre-Check, a program that uses information known about passengers—often frequent flyers, government employees, and others who are assumed to pose little or no risk—to allow them to be screened rapidly at a pre-9/11 level, thereby allowing airport screeners to devote more attention to the other passengers.

Random screening. Given the high volumes of passengers and other limiting factors, an aviation model of security cannot realistically be adopted for surface transportation. However, a number of transportation operators have adopted random passenger screening in which some of the passengers entering a train or subway station are mathematically selected for inspection. Obviously not as thorough as 100-percent screening, random screening offers some deterrent value and provides a platform and training to conduct more-rigorous screening should that be considered necessary on the basis of intelligence.[24]

Random screening offers some deterrent value and provides a platform and training to conduct more-rigorous screening should that be considered necessary on the basis of intelligence.

An MTI study of selective passenger screening concluded that selective searches theoretically can contribute to deterrence, oblige terrorists to take greater risks, complicate their planning, and potentially divert them to less-lucrative venues. The study made no attempt to quantify these effects. It noted that the introduction of any passenger-screening program, especially one that involves selection, runs against Americans' preference for security that is passive and egalitarian, and therefore screening programs must be carefully planned and closely

managed to reduce the inevitable allegations of discrimination or profiling based upon race or ethnicity. The study warned that legal challenges should be anticipated.

Public surveillance. Public surveillance includes CCTV, license-plate readers, facial-recognition systems, and other technology to identify persons, verify identity, detect suspicious behavior, diagnose situations, identify and track down escaping attackers, and prosecute offenders. CCTV provided security authorities with additional eyes and greatly expanded their ability to remotely monitor larger areas. The use of cameras for law enforcement purposes started in the United Kingdom in 1986 with the deployment of three cameras intended to be used for crime prevention. In response to the IRA terrorist campaign, the United Kingdom eventually deployed thousands of cameras in the Underground and on streets.

The first CCTV cameras were costly and crude, but subsequent generations were cheaper and provided better images. Operators also were able to pan areas under surveillance, tilt the cameras, and zoom in on items of interest. Camera surveillance enabled authorities to diagnose situations and identify individuals of interest, eventually achieving a sufficiently high resolution for forensic use in prosecutions.

The problem of monitoring thousands of cameras was eased by the development of analytics built into the software. Alarms on perimeters or at portals immediately brought images from those cameras onto the display panel. Cameras could be programmed to watch for movement where there was not supposed to be any or the absence of movement (e.g., abandoned parcels) where there was supposed to be some. As the analytics improved, cameras became smarter and were able to train themselves. The system would watch for days, identify patterns, and then report anomalies—vehicles going the wrong way or arriving at a time when there were usually none. The most recent systems embed the analytical capability in the camera itself, making it, in effect, a computer with a lens.[25]

The notion that people are constantly under surveillance has raised civil-liberty concerns. But is CCTV effective in reducing crime? Critics charge that law enforcement exaggerates the utility of CCTV and that, in fact, CCTV has proved to be of little or no utility in crime reduction—they claim that, at most, it merely moves crime from heavily surveilled areas to areas with fewer cameras. However, a number of studies carried out in the United Kingdom—which probably has the highest number of cameras per capita of any nation—Sweden, and elsewhere conclude that CCTV does make a modest, but significant contribution to crime reduction. It appears to have some deterrent effect in specific areas such as enclosed environments, public transport, and, most of all, car parks.[26] The significant reduction in vehicle crimes in car parking lots, however, also may be due to better lighting and fencing.

A number of studies...conclude that CCTV does make a modest, but significant contribution to crime reduction.

CCTV also facilitates rapid analysis of situations and interventions. The paucity of camera coverage in Tokyo's subways limited the authorities' ability to rapidly diagnose the situation and identify some type of poisonous gas as the source of an attack with nerve gas in 1995. Since that time, the deployment of CCTV cameras in Japan has proved extremely helpful in identifying and apprehending criminals.

It is more difficult to assess the effects of CCTV on terrorism, because of the low volume of terrorist activity. The terrorists planning the bombing of a New York subway station in 2004 were aware of CCTV coverage and tried to disguise themselves in a way that would not attract attention; CCTV did not deter their attack.[27] The terrorists carrying nerve gas into the Tokyo subway in 1995 and the 2005 suicide bombers in London were photographed entering the stations. As would be expected, CCTV does not deter suicide attackers.

However, British authorities were able to use video footage to ascertain that the 2005 bombing in London was a suicide attack—there were no attackers still at large. In 2006, terrorists planted bombs in two suitcases and left them on German trains. The devices failed to detonate. German authorities quickly located video footage of the two with their suitcases entering a train station and published their photos on national television. Fearing arrest, one fled the country, and the other was quickly apprehended. In the 2013 bombing in Boston, investigators quickly assembled footage from public and private surveillance cameras and were able to publish blurry photos of two suspects within three days. This put the attackers on the run, preventing them from carrying out more attacks that they had planned.[28]

Disarming terrorists. A number of laws and other controls aim at preventing terrorists from easily acquiring weapons and explosives and at facilitating subsequent investigations. Dynamite was readily available for purchase with little scrutiny in the United States in the 1970s. During that decade, the country experienced hundreds of bombings a year. Some of these were related to labor disputes or activities by organized crime; in many cases, dynamiting was simply a means of settling personal scores. But a significant number fell in the category of terrorist bombings. Since then, security at places where explosives are stored and controls on the purchase of explosives have increased. Commercial sources of the ingredients of improvised explosives are also more cognizant of unusual purchases. Although still possible, it is far more difficult now to acquire explosives or significant quantities of chemical ingredients that may be used in explosives without attracting attention.

It is far more difficult now to acquire explosives or significant quantities of chemical ingredients that may be used in explosives without attracting attention.

Controlling access to guns in the United States has been more difficult. Denying the right to acquire firearms (considered by many to be a basic right guaranteed by the U.S. Constitution) solely on the basis of suspicion is opposed by gun-rights advocates and even by some civil libertarians who are less enthusiastic about private gun ownership but who consider any restrictions without due process a threat to individual freedom. Some restrictions have been placed on assault-style weapons and large-capacity magazines. Those arguing for greater gun controls have to concede that terrorists in Europe, where gun ownership is far more restricted than it is in the United States, have been able to utilize their access to criminal networks to obtain fully automatic weapons like those used in the devastating November 2015 terrorist attacks in Paris.

A major problem is the volume of weapons. Weapons are widely manufactured, and most of the world's 875 million small arms are reportedly already in civilian hands.[29] Moreover, rifles and pistols can be used for decades. Large quantities of military-design weapons like

AK-47s are transferred from war zone to war zone. Commercially available non-automatic versions of automatic weapons can easily be converted to fully automatic operability, although that is not necessary for to carry out mass killings. In 2016, the terrorist shooter at a crowded nightclub in Orlando, FL, used a commercially available semi-automatic rifle to kill 49 people and wound 53 others. In 2017, the terrorist shooter at a crowded nightclub in Istanbul used a fully automatic AK-47 to kill 39 people and injure 70.

Small-arms ammunition can be traced through a stamp on the cartridge base, which follows an international standard. This stamp indicates the manufacturer and year manufactured, and some stamps also allow the facility selling the ammunition to be identified. These stamps can be an investigative tool, but, again, the problem is volume—7 billion to 10 billion rounds of small-arms ammunition are sold annually in the United States alone.[30]

In response to the numerous terrorist and other criminal bombings in the 1970s, the Bureau of Alcohol, Tobacco and Firearms sponsored research on taggants. These were materials—microscopic tags—that could be added to commercial explosives at the time of manufacture and would assist in the prevention and investigation of bombings. Detection taggants were designed to signal the presence of explosives to various detection devices. Identification taggants were microscopic objects—for example, tiny spheres—which would survive an explosion and could be easily recovered afterwards by investigators. In one such technology, multiple layers of colors in a microscopic sphere would provide a code that identified the manufacturer and, with proper bookkeeping, the record of the material as it passed through the hands of distributors and merchants down to its purchase or theft.[31]

Although the technology was available, many questions remained about feasibility, safety, costs, and ultimate effects, as explosive devices could be improvised with a variety of materials. Gun-rights advocates also voiced objections, since some gun owners purchased gunpowder to load their own shells. Ultimately, the huge volumes of explosives used and the costs of the technology and record keeping killed the idea of using taggants. In 2014, for example, the United States used more than 3 million tons of commercial explosives (primarily ammonium-nitrate based).[32]

Governments have placed restrictions on the use of ammonium-nitrate fertilizers, which are regularly used as an explosive ingredient when mixed with diesel fuel in large truck bombs like the one used in the 1995 Oklahoma City bombing. In some countries, sale of the fertilizer is banned. Several proposals have been made to add ingredients that render the material less explosive.

***Detection technology*.** Systems for finding weapons, explosives, or the presence of dangerous chemicals have been installed at airports and train stations, on city thoroughfares, and at checkpoints. Metal detectors and x-ray machines have been used to screen passengers at airports for more than 40 years. In addition to metal detectors, screening checkpoints now have full-body scanners that detect not only metal, but other objects and even perspiration. Different technologies have been developed that improve the images provided by the x-ray machines. Objects of different densities are displayed, and the operator can view objects from different angles and zoom in on items of interest.

Airliner sabotage accelerated efforts to develop reliable explosives-detection technology. A major impediment to aviation security was the need for a system that could rapidly examine large volumes of objects quickly, with a near-zero false-negative rate and a low false-positive rate. The President's Commission on Aviation Security and Terrorism (1989–1990), convened after the 1988 sabotage of PanAm flight 103 in which 270 people were killed (11 of whom were on the ground), recommended that the Federal Aviation Administration foster the development of explosives-detection technology;[33] however, a subsequent review by the Congressional Office of Technology Assessment recommended that deployment of existing systems be delayed because promising technological developments were expected to soon produce more-reliable systems.[34] Following the 1996 crash of TWA flight 800, which was at first suspected to have been caused by a bomb, the White House Commission on Aviation Safety and Security (1996–1997) recommended the deployment of the new systems.[35] The airline industry generally opposed this recommendation, and it was not until after 9/11 that the federal government mandated that all baggage be screened.

New systems using a variety of technologies have been deployed to detect explosives. Bulk detection focuses on imaging characteristics. Trace detection relies on detecting tiny amounts of vapors emitted by explosive compounds. In addition to the technologies in development or in use, canines are still effective in detecting tiny quantities of chemical vapors. More recently, dogs have been trained to detect vapor wakes; that is, instead of sniffing persons or objects, dogs may be able to detect vapor trails by sniffing the air that somebody carrying a bomb has walked through.

More recent efforts have aimed at stand-off detection, that is, detecting explosives carried in vehicles or on persons at a distance sufficient to allow early intervention. Some behavioral techniques to detect suicide bombers are in place now, and new technology allows operators to detect an individual carrying a bomb in a crowd. The tactical challenge is how to defuse the threat without increasing the danger to people in the surrounding area.

Police, soldiers, and guards. Visible (and undercover) security personnel have been deployed to deter terrorist attacks, detect suspicious behavior, and provide an immediate response if an attack does occur. In response to the growing threat of random attacks, officials in London launched a program called "Project Servator" in 2014. The program consists of new policing tactics involving a highly visible but unpredictable police presence, behavioral-detection techniques, and random checks to deter and detect criminal and terrorist activity and to reassure the general public.

Anecdotal information indicates that the presence of police or security personnel can have a deterrent effect. The heavy presence of police and other security personnel in the Paris Metro and commuter train stations following a bombing at an underground station in 1995 appears to have persuaded the terrorists, who were still at large, to place their bombs at the entrance to the station or select other targets where they were less likely to encounter security personnel. In the 2006 attempt to bomb commuter trains in Germany discussed earlier, the bombers had planned to carry their suitcases containing bombs on an earlier date but decided to delay their attempt when they saw that the train stations were filled with police—the German government had deployed the added personnel to protect the

World Cup matches then taking place. The terrorists placed their bombs on the trains at a later date. Fortunately, the devices malfunctioned and no explosions occurred.[36] In the November 2015 terrorist attacks in Paris, three bombers who intended to enter a football stadium were prevented from doing so by a single security guard. The bombers detonated their devices outside of the stadium, killing only themselves.[37]

Inner perimeters and access control. Terrorism contributed to the proliferation of inner perimeters protected by access-control systems designed to prevent terrorist access to specific facilities or zones. In medieval times, castles restricted the flow of visitors through barbicans—narrow passageways to funnel visitors (or attackers) through obstacles and "dangers" controlled by the defenders—gatehouses, and portcullises, all manned by armed guards. Over time, the technology has changed. Advanced access-control systems with locked doors, turnstiles, badges, and card keys became increasingly common in the 1960s as a response to crime. Terrorist bombs, often placed at corporate headquarters in the 1970s, led to the acceleration of access control in the subsequent years. Some type of access control is now in place at most federal government buildings and many corporate offices, commercial properties, and residences. More-advanced security systems use biometrics to ascertain identity.

Zone defense and "rings of steel." The difficulty of protecting soft targets in cities led to the implementation of zone defenses, or so-called "rings of steel." These are intended to deny terrorist access to entire zones of a city. The first "ring of steel" was created in the 1970s in response to the IRA bombing campaign in Belfast, Northern Ireland. Between 1970 and 1975, 1,800 bombs destroyed 300 business establishments in the city, comprising one-quarter of the commercial floor space. In 1972, Belfast's commercial center was surrounded by a fence, which shoppers could enter through checkpoints where parcels were inspected for bombs. Vehicle access and parking were restricted. In 1974, the fence was replaced by a more elaborate and permanent array of defenses. Gradually, the IRA shifted its sights to other targets. The barriers were gradually removed, and the security measures were relaxed in the 1980s, but a centralized CCTV system was implemented in 1995.

The difficulty of protecting soft targets in cities led to the implementation of zone defenses, or so-called "rings of steel."

In 1992, a massive truck bomb detonated by the IRA destroyed the Baltic Exchange building in London's financial district. Three people were killed, and the bomb caused $1.2 billion in damage. This led to the imposition of new security measures, including roadblocks and vehicle checks. When these measures were relaxed in 1993 to facilitate the flow of construction vehicles involved in rebuilding the Exchange, the IRA struck a second time, bombing the Bishopsgate area, killing one person and causing $1.5 billion in damage. In response to this attack, a "ring of steel" was erected around the city. Vehicular access to the city was sharply restricted, entering vehicles were searched at checkpoints, and CCTV was installed at every checkpoint. A "collar zone" consisting of increased police presence and random checks surrounded the "ring of steel." These measures were gradually reduced after the IRA agreed to end its terrorist campaign in 1998, but they were reactivated after 9/11. The current system, which is referred to as the "ring of glass," relies

more on domain awareness achieved through CCTV coverage and a heightened police presence. The "ring of steel" did halt further bombings within the city of London, but IRA terrorists carried out large-scale bombings outside the ring and in other British cities.

In response to the Second Intifada, the terrorist campaign that resulted in thousands of terrorist attacks and more than a thousand Israeli deaths between 2001 and 2008, Israel initiated a number of extraordinary security measures, including starting construction of a security barrier—a wall that would be 790 kilometers long if completed. This barrier has made infiltration by terrorist bombers much more difficult, but some Israeli officials credit the decline in bombings to the effective actions of the Israeli intelligence services, which infiltrated the terrorist groups and disrupted their operations.

The devastating economic impact of the 9/11 attacks and fears that major financial institutions would relocate to other areas, resulting in loss of tax revenues and high unemployment, prompted New York City to create the Lower Manhattan Security Initiative. Authorities judged this to be more efficient than trying to protect individual properties. New York's "ring of steel" was, in fact, a "ring of glass," more surveillance than physical barriers. Although it included some traffic restrictions and checkpoints, it consisted primarily of several thousand security cameras, license-plate readers, facial-recognition technology, and sensors to detect explosives, chemicals, biological pathogens, and radiation; it was supported by the latest analytical technology, aimed at rapid detection, diagnosis, and disruption of possible terrorist attacks. Additional checkpoints and other security measures monitored vehicles coming into Manhattan.

New York's "ring of steel" was, in fact, a "ring of glass," more surveillance than physical barriers.

These special security zones have had some positive benefits. They may have had some deterrent effect, at least diverting attackers to other, less-strategic targets away from city centers. They protect vital commercial institutions and activities. They have arrested or reversed declines in retail commerce owing to insecurity. They probably persuaded some corporations and retail commerce not to relocate, thereby saving population, jobs, and revenue. (Economists may argue that relocation would replicate the jobs and revenue elsewhere.) Finally, they have created safe environments for residents and workers—many feel that they have reduced traffic and increased a sense of security.

The role of illusion. Critics sometimes dismiss security measures as nothing more than show, but what may appear to critics to be a charade may not be assessed the same way by terrorist operatives who look not at the imperfections, but at the remaining risk. The shortcomings of a security regime may be obvious, but terrorists who may have only one chance to succeed and for whom the consequences of failure are significant may view even a low risk of detection as too dangerous. Security measures are designed to affect the perceptions and calculations of the attacker as much as they are to prevent an actual attack.

What may appear to critics to be a charade may not be assessed the same way by terrorist operatives.

***Design features and construction materials*.** The use of specific design features and construction materials is aimed at strengthening structures against catastrophic failure, mitigating casualties, and facilitating surveillance and evacuation. In April 1983, a truck bomb destroyed the American embassy in Beirut. The Iraqi and French embassies in Beirut already had been the targets of previous vehicle bombs in 1981 and 1982. The Beirut attack was followed by a suicide terrorist bombing of the American embassy in Kuwait in December 1983, and the French embassy there was bombed the same day. In 1984, terrorists bombed the American embassy annex building north of Beirut. In response to these bombings, barricades were hastily erected around buildings in Washington, D.C., and dump trucks were parked at the gates on the driveways into the White House. The Secretary of State's Advisory Panel on Overseas Security (the Inman Panel, named after its chairman, Admiral Bobby Inman), convened in 1985 to review the security of diplomatic personnel and facilities overseas, made a number of recommendations, including a massive rebuilding program to improve the security of American diplomatic facilities.[38]

At the same time, the U.S. Department of State convened a Committee on Research for the Embassy of the Future. The committee's charge was to establish new design and construction specifications for diplomatic facilities abroad. The major challenge was that of dealing with massive truck bombs. To withstand the blast effects of some the largest truck bombs would require the construction of World War II–era fortifications, which was impractical. Instead, the committee recommended setbacks from thoroughfares and construction of barriers to keep explosions at a distance; however, these actions were not always possible in urban areas. Combinations of setbacks and more-robust construction techniques and materials could mitigate the effects of large truck bombs, but residual risks would remain.[39]

Terrorist bombings gave impetus to research that led to further improvements in building materials and especially in glazing (explosions could turn windows into deadly shards of flying glass). Engineers developed sophisticated computer programs to measure the effects of different types and weights of explosives at varying distances. In some cases, windows were deemed impractical. A 187-foot concrete base was added to One World Trade Center—the Freedom Tower, which replaced the twin towers of the World Trade Center—to diminish possible casualties from shockwaves that would ascend the structure from a bomb at street level.

Prior to 9/11, public surface-transportation operators gave little attention to crime prevention through environmental design (CPTED), but a survey conducted in 2005 indicated that 80 percent of operators believe that CPTED can play a useful role.[40] New train-station construction in the United States and Europe features open spaces that facilitate surveillance, reduce the effects of explosions, and eliminate sources of shrapnel.[41]

Enlisting the public's help. Public-awareness campaigns that enlist the public to "see something, say something" are a logical response to random terrorism. They have existed in their current form for 25 years. Faced with IRA attacks on public transportation, British authorities sought the assistance of staff and passengers in identifying suspicious objects. The IRA's terrorist campaign imposed a staggering burden on transportation security and a nervous public. Between 1991 and 1997, there were 41 IRA attacks on transportation

targets in England involving 81 devices and 29 explosions. In addition, there were 6,569 telephone bomb threats. Of the 81 explosive devices placed at transport targets, 79 were hand-placed time bombs, 50 percent of which did not work as intended. Altogether, only three people were killed by IRA bombs on the rail system: one at Victoria Station in 1991 and two on the Docklands Light Railway in 1996. This low number of casualties, however, is not due solely to the great pains taken by the terrorists to avoid casualties. Without a prompt response to threats, the death toll could have been much higher. Killing, however, was seldom the IRA's primary objective.[42]

Public involvement was critical to the security strategy in England, despite its limitations and the risks of false alarms, especially immediately following terrorist attacks. Signage and repeated public announcements kept the public alert to the terrorist threat and to the need to keep personal packages under direct control, to remain vigilant for left parcels, and to immediately report suspicious activity or articles to staff. The police remained confident that any left parcels would be discovered in minutes, and because most IRA bombs were set with an hour or more on the timer, police would have time to respond.

It was not enough to merely advise the public to be vigilant. Passengers had to have a readily available means of communication—this was an era before people carried mobile phones. British Transport established "help points," telephones, and emergency alarms. Passengers were instructed about what constituted an emergency and were encouraged to use the help points and alarms when appropriate. CCTV cameras covered the help points and alarms so that staff could see who was calling and why. The third essential ingredient was visible response. Passengers notifying the authorities could not be ignored, but had to see some action in response to their concerns. Between 1991 and 1997, 9,430 suspicious objects were reported and investigated. The Underground and railroads also had to deal with more than a quarter-million lost or abandoned items every year, any one of which might have been a bomb.[43]

This is one of the few security measures for which it is possible to quantify results. Using the MTI database, researchers looked at worldwide patterns in attacks aimed against buses, trains, and passenger ferries and found that in 300 incidents—just under 9 percent of all attacks on these targets—alert citizens, passengers, or officials thwarted an attack by discovering bombs before they could be detonated. In approximately 43 percent of these cases, the individual who found the device was not identified. But in about 17 percent of the incidents, the device was found by alert passengers or citizens; in about 13 percent, the device was discovered by security or intelligence officials; in about 15 percent, military or police found the device; and in about 11 percent, the device was discovered by alert transit drivers, crew, or employees.[44]

In 300 incidents—just under 9 percent of all attacks on these targets—citizens, passengers, or officials thwarted an attack by discovering bombs before they could be detonated.

The same pattern generally holds in Europe, where a slightly higher percentage of attacks—11 percent—were foiled because bombs were detected. In 51 percent of these discoveries, the original source of information that prompted action is unknown. Where

more data are available, it is known that transit employees and drivers found devices in 20 percent of the prevented attacks, passengers and citizens found them in 12 percent of the attacks, security officials or intelligence found them in 7 percent, and police found them in 10 percent.[45]

Turning, finally, to the 12 attacks on surface transportation in Canada and the United States, three (25 percent of the incidents—the highest percentage so far, although the number is very small) involved devices that were found before detonation. One was found in a passenger train, one in a subway station, and one in a train station. In the train-station case, in 1992, a maintenance worker found a grenade.[46]

Toward earlier intervention. Is it possible to push back the moment of detection of terrorist intent, enabling earlier intervention? This is a quest of current research. It focuses on the narrow time frame between the final commitment to action when the armed perpetrator is on the way or already at the selected target and poised to attack and the attack itself. Faced with a campaign of suicide bombings, Israeli security personnel were trained to watch for telltale signs of dress or comportment that indicated a possible suicide bomber. Since many of the bombs were being detonated on crowded buses, Israeli bus drivers were instructed about suspicious behavior to watch for as they approached bus stops and when to drive by rather than risk boarding a bomber.[47]

Behavioral detection operates on the premise that subtle indicators of possible criminal intentions—displays of nervousness or apprehension, for example—can be detected by trained observers. Skillful intervention, even a casual approach, may trigger further indicators. However, this is a controversial area. In 2013, the Government Accountability Office found that there was no evidence to back up the idea that "behavioral indicators … can be used to identify persons who may pose a risk to aviation security." After analyzing hundreds of scientific studies, the investigators concluded that "the human ability to accurately identify deceptive behavior based on behavioral indicators is the same as or slightly better than chance."[48]

Critics charge that behavioral detection works only because it is thinly disguised racial profiling—more African Americans, Hispanics, and persons of Middle Eastern appearance are stopped because it is believed that they are more likely to have outstanding warrants or immigration violations or be carrying drugs or weapons. This contention gained credence when some behavioral-detection officers at Boston's Logan Airport, where a pilot program was being tested, complained that co-workers resorted to racial profiling to improve their numbers.[49] Others disagree, arguing that when properly used, behavioral detection is a legitimate and useful technique.

New technology offers a mechanical approaches. A subject checking in at a kiosk may receive a subliminal prompt—an image or phrase—designed to provoke an emotional reaction that is then assessed by an embedded camera photographing the subject. Other research efforts are combing video footage of criminal assaults to see if there are telltale patterns of behavior just prior to the assault that could be programmed into surveillance cameras and used to alert police.

Whether they actually work or not, behavioral-detection efforts may have some deterrent effect. Long before airline passenger screening was implemented, U.S. authorities claimed to have the ability to identify would-be hijackers. They did not have that ability, but some potential hijackers believed that they did. There is no way to know how many hijackings may have been deterred by this tactic.

V. DOES SECURITY WORK?

Shoplifting is a crime that occurs frequently, and new technology allows inventory shrinkage to be monitored easily and measured accurately. That offers a reliable base line. As a result, the effects of security measures involving CCTV or electronic merchandise tags can be rapidly determined, and calculations even can be made about how long it will take to amortize the cost of the system against the losses incurred. In contrast, it is much harder to keep score in the domain of terrorism. There are no easy metrics.

SECURITY MEASURES BY THEMSELVES HAVE NOT REDUCED TERRORISM

There has been no reduction in the total volume of terrorism worldwide, nor is it reasonable to expect any. As indicated already, most terrorist activity is concentrated in conflict zones, where it is one dimension of ongoing warfare. Outside of these conflict zones, terrorist attacks occur only rarely. Going back to the statistics cited earlier, according to the GTD, in the past 15 years, roughly 27 percent of the world volume of terrorist activity—roughly 23,000 incidents—took place outside of conflict zones. That sounds like a lot, but spread over 15 years, it comes to about 1,500 attacks a year. Divided by more than 100 countries where terrorist attacks have occurred, the average is about 15 attacks per country each year. If this is further divided by target sets to gauge the effects of different security regimes, the numbers are even smaller, and the effects may take decades to discern, making statistical analysis difficult.

The effects may take decades to discern, making statistical analysis difficult.

In Europe and the United States, the volume of terrorist violence is generally lower than it was in the 1970s, although this decline is mainly the result of ending some of the armed struggles—in particular, the IRA's 25-year terrorist campaign and a reduction of the Basque separatist violence in Spain—and the successful suppression of earlier terrorist groups such as the Red Army Faction in Germany, the Red Brigades in Italy, *Action Directe* in France, and the Weather Underground and other neo-Marxist groups in the United States. Other groups have just disappeared.

Better security and stricter controls on commercial explosives and the ingredients of improvised explosive devices have also contributed to the decline in the number of terrorist bombings, still the most common terrorist tactic. New laws have facilitated intelligence collection and broadened police powers, increasing the likelihood of identifying and apprehending perpetrators.

The Palestinian organizations and their allies that were responsible for a number of terrorist attacks in Europe in the 1970s and 1980s were also gradually contained. Clearly, increased security made some of their favored tactics, e.g., airline hijackings and assaults on embassies, more difficult, but other factors also contributed to the decline. However,in the past 15 years, terrorists motivated by jihadist ideologies have carried out spectacular attacks in Madrid, London, Paris, Brussels, and Nice. The volume of attacks may be less than in the 1970s, but random targeting and the scale of carnage make these the main drivers of security today.

The declines are often hard to demonstrate statistically, as the total numbers, especially of incidents with fatalities, are so low to begin with. In any graph, the line bumps along the bottom. Only when examined over the very long run—decades—does the trajectory become apparent.

In the 15 years between September 12, 2001, and December 31, 2016, homegrown terrorists inspired by jihadist ideology carried out only 16 terrorist attacks in the United States; the number rises to a few dozen if attacks by other domestic extremists are added.[50] This is not a complaint about a terrorism deficit. Having only two or three events a year is very good news for the country, but it makes an empirical evaluation of security measures difficult.

Having only two or three events a year is very good news for the country, but it makes an empirical evaluation of security measures difficult.

One way to measure the effectiveness of security against terrorism is to look at attempts by terrorists to directly overcome defenses by mobilizing more attackers, employing heavier weapons, or using suicide tactics. Escalation would indicate that terrorists were being forced to increase their investment. But terrorists launch very few direct assaults on defended targets outside of conflict zones. Resource constraints limit their ability. The growing volume of terrorism worldwide has not seen a parallel increase in the scale or intensity of armed confrontations with security forces other than those responding to attacks. The lack of examples of terrorists attempting to directly overcome security indicates that terrorists have ample easier options. Their attacks are aimed at killing as many civilians as possible before the terrorists themselves are surrounded and killed by security forces. The 2008 attack in Mumbai, the 2013 attack on the Westgate Mall in Nairobi, and the 2015 attack in Paris are examples.

There are also very few examples of terrorists employing heavier weapons. They rarely have access to weapons such as artillery or armored vehicles. Moreover, the requirement to operate clandestinely and to conceal their preparations works against the use of heavy weapons even if they had them. The terrorists would lose the element of surprise. Terrorists in the 1970s operated with readily available firearms and the arsenal of light infantry—pistols, semi-automatic assault rifles, AK-47s. Today's terrorists use the same weapons.

One development apparent in earlier decades, however, was the increased use of standoff weapons, including mortars and rocket launchers, which enabled terrorists to engage their preferred targets at a distance without directly confronting security forces. Another development was the use of larger and larger truck bombs, which could be rammed through defenses by suicide drivers or could cause massive damage to a target even if detonated at a distance.

Suicide attacks, which may be seen at least in part as a response to security, have become more prevalent and are now part of the terrorist repertoire in both Europe and, to a lesser degree, the United States. This is a response to security, but it also can be viewed as a security success of a sort, since suicide is a high threshold and suicide attackers are harder to recruit.

Again, as noted above, terrorists do not need to increase the size and weapons of their attacking force or their death wish to solve security problems. Terrorists do not double down and they rarely give up—they adapt. They can solve almost any security challenge by merely changing their target from one that is heavily defended to one that is hardly defended at all. That means that security measures are more likely to displace risk than to prevent an attack. Faced with security measures at a particular target, the determined terrorist selects another target. This generally has been the pattern.

One obvious measure of the effectiveness of security is missing. Almost no terrorist attackers are foiled at security perimeters. Airport screeners in the United States discover thousands of weapons forgotten or concealed in carry-on luggage, but they have not caught a single hijacker. They have discovered no bombs on would-be saboteurs. This is pretty much true worldwide. Very few terrorists are caught at perimeters or security checkpoints. But the question of how many terrorists have been caught by security measures may be irrelevant. The paucity of failed terrorist attempts (other than incidents of explosive devices that fail to detonate, which is a technical problem) suggests that terrorists determined to carry out an attack select tactics and targets that virtually guarantee success.

Almost no terrorist attackers are foiled at security perimeters.

MEASURES SHOULD PROVIDE A "NET SECURITY BENEFIT"

The ability of terrorists to select less-protected targets raises an important issue. In some circumstances, displacing the risk of a terrorist attack even temporarily is worthwhile. Important national and international events merit special security even without the expectation that it will prevent terrorist attacks elsewhere. But as a general rule, security measures, especially those that are disruptive or costly, should do more than merely move terrorists down the street.

Commercial aviation is protected by extraordinary security measures for good reasons. Sabotage of an airliner in flight can result in hundreds of fatalities. A terrorist takeover of an airliner poses potentially even greater dangers. The 9/11 attacks offer the most compelling example. There is, therefore, a net security benefit to preventing weapons and explosives from being carried onto airplanes. Protecting nuclear facilities, dangerous materials, certain components of the infrastructure, and political leadership also offers net security benefits to society.

There is...a net security benefit to preventing weapons and explosives from being carried onto airplanes.

Security in the public areas of airports is a different story. People at check-in and baggage-arrival areas have been the targets of terrorist attacks, and security has been increased in some of these areas, but it is not clear that new security perimeters at the entrance to terminals offer much of a net security benefit. Screening at terminal entrances creates new bottlenecks; crowds waiting to get in become tempting targets.[51]

This can be seen in a terrorist attack in Turkey. In response to a heightened terrorist threat, a security checkpoint was erected at the entrance to Istanbul's airport to screen passengers

coming into the terminal. The original checkpoint inside the terminal continued to screen passengers before they boarded their flights. In June 2016, two terrorists opened fire as they reached the first security perimeter, killing 41 people and injuring more than 200. A third attacker detonated a bomb in the adjacent parking lot. In a sense, however, Istanbul's security measures worked: Although the shooting at the front door was not prevented, it allowed passengers inside to flee—worse casualties might have occurred if the terrorists had been able to slip unnoticed into the busy terminal.[52] Further terrorist attacks in the publicly accessible portions of airports no doubt will increase pressure to increase security in terminals, but it is a more difficult challenge than passenger screening.

Crowds waiting to go through security checkpoints at train stations are also vulnerable, as demonstrated in a December 2013 terrorist attack in Volgograd, Russia, where a suicide bomber detonated his device just before the security checkpoint that had been installed at the entrance to a train station, killing 18 and injuring at least 44.[53]

Finally, if deprived of the opportunity to attack airports and train stations, terrorists still have many other public places where an armed assault or explosion could achieve similar results—shopping malls, supermarkets, theaters, restaurants, nightclubs, tourist sites, busy streets, and other places of gathering. The security investment and the disruptions caused by attempting to secure these places would be significant, while the net gains would be slight. Another checkpoint cannot be the response to every attack in a public area.

Another checkpoint cannot be the response to every attack in a public area.

SECURITY MEASURES ALSO SERVE FUNCTIONS OTHER THAN PREVENTION

While the ultimate purpose of security measures collectively is to deter or prevent attacks, not all such measures have a directly preventive function. Physical barriers may be designed to delay attackers and alert responders. CCTV surveillance may discourage criminal activity, but it does not prevent all attacks. Other measures facilitate surveillance or mitigate effects. Security measures work in concert, and it is difficult to judge the positive effects of any single one. Can we instead judge incidents where security has seemed to fail?

WHY DOES SECURITY SO OFTEN SEEM TO FAIL?

Almost every terrorist attack is seen as a failure of security. But this is hardly the right way to assess the effectiveness of security measures. As noted above, about 80 percent of the terrorist attacks to date have been directed against targets where there was no security. Security cannot be said to have failed where it does not exist. In roughly another 10 percent of the attacks, the security circumstances are unknown. These are, to be sure, judgment calls based upon interpretation of a limited statistical sample of terrorist events, but it would appear that in only about 10 percent of the attacks did the attackers encounter some form of security.

Terrorists rely upon stealth or surprise to succeed. In some cases, terrorists stormed their targets by force of arms or blew themselves up as they neared checkpoints, but most of

these types of attacks took place in conflict zones and are not typical of terrorist attacks in other areas. This is an intriguing area worthy of further study.

TERRORISTS SUCCEED BY ATTACKING UNPROTECTED TARGETS AND BEING WILLING TO DIE

A closer look at the jihadist terrorist attacks that have occurred in the United States in the past 15 years offers some insights into the issue of security failures. The 9/11 attacks reflect several failures. Intelligence indicated that al Qaeda's terrorists were planning to do something, but the investigators were unable to identify the specific plot. They also failed to follow up on leads that would have led them to some of the attackers. Ten of the 19 hijackers were identified by CAPPS and should have been subjected to extra scrutiny at the checkpoints. However, because of the way the system was configured, their selection by CAPPS had little operational meaning at the checkpoints. Whether the hijackers smuggled their weapons on board remains a matter of dispute. Passengers phoning from the hijacked flights mentioned box cutters, knives, and some form of Mace or pepper spray. The airlines have maintained that box cutters and knives with blades of the length the hijackers were known to have purchased were not prohibited. Others contend that they were. Any kind of Mace or pepper spray was clearly prohibited, but it is not proven that the terrorists had these items. The consensus view, however, is that passenger screening had clearly failed, so the federal government took over airline security.

Most of the jihadist terrorist attacks in the United States since 9/11 have been shootings, and almost all of the victim deaths were the result of gunfire. Terrorist attacks with guns include the 2002 attack at LAX; the 2009 shootings at a military recruiting office in Little Rock, AR, and at Fort Hood, TX; the 2015 shootings in Chattanooga, TN, Garland, TX, and San Bernardino, CA; and the 2016 shooting of policemen in Philadelphia, PA, and at a nightclub in Orlando, FL. Several of the assailants had previously been on the radar or under surveillance as possible terrorist suspects, making their attacks a "failure" of intelligence, but thousands of people come onto the radar, while only a handful ever carry out attacks. Dangerousness is difficult to predict.

Most of the jihadist terrorist attacks in the United States since 9/11 have been shootings, and almost all of the victim deaths were the result of gunfire.

In all of the shootings except for the one at Fort Hood, the assailants did not have to penetrate any security perimeters or pass through any checkpoints. They carried out their attacks in public places, although they could expect that there would be a rapid armed response, which did occur in almost every case. The shooters in Chattanooga, Garland, and Orlando were all taken under fire and killed at the scene. The attackers in San Bernardino were killed in a gun battle with police hours later. The attacker in Philadelphia was shot and wounded at the scene. At Fort Hood, the attacker was a senior army officer with identification who was able to enter the facility, where he opened fire on his fellow soldiers. He, too, was shot and wounded.

Three of the attacks in the United States since 9/11 involved bombs: the 2010 attempted bombing in New York's Time Square; the 2013 bombing in Boston, MA; and the 2016 bombing in New York City. The New York City bomber had also placed an improvised explosive device in New Jersey, but it failed to detonate. The bombs were all placed in public areas, and all of the bombers were quickly identified and arrested or killed by police.

In two of the remaining cases—in Merced, CA, in 2015, and St. Cloud, MN, in 2016—the attackers stabbed their victims; in another 2015 case, an assailant attacked policemen with a hatchet. In 2016, an attacker rammed his vehicle into pedestrians and then attacked them with a knife. In yet another incident, an individual simply rammed pedestrians with his automobile in 2006. Again, these attacks took place in public areas, although the attackers could expect an armed response—four were killed by police, and the fifth, the driver of the automobile in 2006—surrendered to authorities immediately after the attack.

In most of the cases, the prospect of immediate death did not deter the attackers. They succeeded not because of a failure of security, but because it was easy for them to attack unprotected civilians, and except for the bombers, most of the attackers were ready to die. That would seem to suggest that terrorists cannot be deterred, but there is evidence that indicates otherwise.

They succeeded not because of a failure of security, but because it was easy for them to attack unprotected civilians, and except for the bombers, most of the attackers were ready to die.

VI. CAN TERRORISTS BE DETERRED?

It is difficult to prove empirically that security has a deterrent effect. We cannot count events that don't occur. The absence of attacks could be attributed to a deterrent effect or simply to the lack of any terrorist intentions to carry out such attacks. We cannot be sure which it is.

However, there is a growing body of research indicating that terrorists take security into account in their planning and that increased security appears to have contributed to altering certain tactics or deterring terrorist attacks against certain categories of targets.[54] Terrorists may be ready to sacrifice their own lives, but they still seek operational success. Part of the allure of terrorism, and of violent jihadist ideologies in particular, is the opportunity to demonstrate not only commitment, but prowess in a warrior subculture. Dying in a failed attempt may still bring individual attackers posthumous rewards, but tactical failures accrue less prestige, and for the organization, strings of failed attacks hardly make effective recruiting posters. Even the most fanatical attackers want to do more than hurl themselves against impregnable walls in futile attempts to breach defenses. The following examples indicate that deterrence seems to have worked or at least contributed to a decline in the use of certain tactics or attacks on certain target sets.

Terrorists may be ready to sacrifice their own lives, but they still seek operational success.

TERRORIST KIDNAPPINGS OF DIPLOMATS DECLINED AS TERRORISTS TURNED TO OTHER TARGETS

Terrorists began kidnapping diplomats in the late 1960s. In the early 1970s, they began kidnapping corporate executives and demanding ransoms as a means of funding their operations. The kidnappings prompted increased security. Personal protection became a major industry involving armed bodyguards, armored cars, defensive driving courses, convoys of protection personnel, increased security at offices, and safe rooms at officials' and executives' homes, along with procedures to protect schedules and alter routes and times of travel.

Terrorist kidnappings overall declined in the later 1970s and early 1980s, but they did not end. Increased security was a contributing factor, but not the only one. In many countries, the urban guerrilla and terrorist groups responsible for the early wave of kidnappings were suppressed. In countries unable to apprehend kidnappers or destroy kidnapping rings, kidnappings continued; both guerrilla groups and ordinary criminals participated in this lucrative criminal activity, especially in Latin America, where kidnappings increased in some countries.

However, instead of targeting the better-protected diplomats and high-ranking political officials, the kidnappers shifted their sights and went after lower-level executives, relatives of prominent individuals, aid workers, missionaries, journalists, and others who had little or no protection. In this context, security worked. There were some striking exceptions, including the kidnappings of prominent German businessman Hanns-Martin Schleyer in 1977, of Italy's former prime minister Aldo Moro in 1978, of American General James

Dozier in Italy in 1981, and of a number of prominent Latin American business executives.[55] Another example—one that did not involve kidnapping—was the 1989 killing of Alfred Herrhausen, the head of Deutsche Bank.

EMBASSY TAKEOVERS SOARED IN THE 1970S, THEN WERE ABANDONED AS A TACTIC

In the early 1970s, terrorists began to seize hostages at embassies and other diplomatic facilities. These incidents differed from kidnappings in that the terrorists knew they would be promptly surrounded by police and military units, but they attempted to negotiate their escape along with the satisfaction of other demands in return for the release of their hostages. Throughout the decade, terrorist takeovers of embassies remained a prominent means of attracting international attention and exerting political coercion. Between 1971 and 1981, terrorists seized hostages at embassies or other diplomatic facilities on 43 occasions and unsuccessfully attempted to storm embassies on five more occasions. In addition, mobs sacked embassies numerous times, and unarmed protesters occupied them, holding hostages.

The tactic appeared contagious. The events occurred in clusters, increasing in the early 1970s, reaching a plateau in the middle of the decade, then dipping before climbing sharply at the end of it. Then the tactic virtually disappeared.

At least part of the decline probably was due to increased security. Embassies turned into virtual fortresses, while host governments increased surrounding security. The five failed attempts to seize hostages at embassies all occurred between 1976 and 1979, reflecting the effectiveness of increased security. Moreover, the countries whose embassies were the most prominent targets of terrorism during this period (Israel, the United States, and Germany) are underrepresented in the takeovers, suggesting that heavy security at these sites, which earlier had been prominent targets of terrorist attacks, encouraged would-be hostage-takers to target the embassies of other countries whose embassies were less protected.

Part of the decline also reflects what happened after the terrorists seized hostages. As the tactic proliferated, governments became increasingly resistant to meeting the demands of hostage-takers anywhere, either aboard hijacked airliners or inside embassies. The hostage-takers saw their demands fully or partially met in 40 percent of the cases in the first half of the decade; the proportion dropped to 25 percent in the second half. Terrorist demands were *fully* met in only 17 percent of the incidents. Evidence of increasing resistance to terrorist demands was also reflected in the growing length of the hostage standoffs.

As the tactic proliferated, governments became increasingly resistant to meeting the demands of hostage-takers anywhere.

As governments became more resistant to terrorist coercion, they also became more willing to use force to end hostage situations whenever possible. Armed rescues of hostages were made by French commandos in Djibouti in 1976, by Israeli commandos in Entebbe in 1976, by German commandos in Mogadishu (where hostages were held aboard a hijacked airliner) in 1978, and by Egyptian commandos in Cyprus, also in 1978. An attempt by U.S.

forces to rescue American hostages held in Tehran in 1980 was aborted when a desert sandstorm disabled several of the helicopters carrying the rescue team.

Host governments dealing with embassy takeovers remained reluctant to risk the lives of foreign diplomats held hostage. In an episode that was an operational and diplomatic disaster, protesters seized control of the Spanish embassy in Guatemala in 1980; despite pleas from the Spanish ambassador to negotiate a peaceful resolution to the incident, Guatemalan forces were ordered to attack. Thirty-six people, including both hostages and hostage-takers, died in a fire started during the assault. The ambassador narrowly escaped. Later in 1980, British commandos successfully stormed the Iranian embassy in London, which had been taken over by terrorists.

Faced with the increasing prospect of encountering heavily armed guards, growing failure to achieve results beyond publicity, and the increased risk of death or capture, terrorists abandoned embassy takeovers. They did not abandon attacks on diplomatic facilities, however; they merely altered their tactics from takeovers to large-scale bombings.[56]

INCREASED SECURITY AND POST-9/11 PASSENGER REACTIONS HAVE MADE TERRORIST HIJACKINGS MORE DIFFICULT

Evidence of deterrence due to security can be found in long-term trends in terrorist hijackings and airline sabotage attempts. Aviation security remains one of the most important components of overall defense against terrorism. In the early 1970s, terrorist hijacking or bombing attempts worldwide were occurring, on average, at the rate of one every couple of months—and people still flew. Since then, the number of hijacking attempts has declined. There were 43 attempted hijackings in the 1970s, 26 in the 1980s, 16 in the 1990s, and 19 between 2000 and 2009, including the four airliners hijacked on 9/11. We cannot claim that the 9/11 attacks were anything other than a terrorist success, but this success conceals the fact that it required four or five hijackers on each plane who were willing to commit suicide—19 in all. Recruiting that many suicide attackers poses a high threshold, beyond the capabilities of most terrorist organizations.[57]

Evidence of deterrence due to security can be found in long-term trends in terrorist hijackings and airline sabotage attempts.

The number of sabotage attempts has also declined. In the 1980s, there were 39 attempts to sabotage airliners. The number dropped to 15 in the 1990s, and to eight in the first decade of this century. Clearly, this was progress, although many factors were driving the decline. In part, the decline reflected the fact that there were fewer terrorist groups focused on aviation. In the 1970s and early 1980s, terrorist hijacking and sabotage attempts were being carried out by a number of Palestinian groups, Shi'ite and Sikh fanatics, Croatian separatists, Ethiopian extremists, Cubans waging war on Castro's Cuba, and members of the Japanese Red Army and Germany's Red Army Faction, as well as Libyan and North Korean agents. A number of these groups were eventually suppressed. Under intense global pressure, others, including the Palestinian organizations responsible for some of the most spectacular hijackings in the 1970s, were persuaded to abandon this tactic.

Another reason for the decline in terrorist attempts against aviation was increasing security. Following the first terrorist hijacking of an El Al airliner in 1968, the Israeli government adopted the most stringent security measures of any airline. There have been no further hijackings of El Al airliners. Terrorists did not give up the tactic, however; they simply targeted other airlines. Yet, as the numbers indicate, these hijackings of also declined over time. Locked, armored cockpit doors and passengers willing to pounce on anyone threatening an airplane have rendered hijackings, if not obsolete, a far riskier tactic for terrorists and one with greater chances of failure. Hijackings today are more likely to involve mentally disturbed persons or individuals claiming to have explosive devices that are invariably hoaxes.

While some critics may think airline security is a charade, and probes by government-sponsored "red teams" have indicated unacceptable rates of failure that must be remedied, terrorists know that security still poses risks to attackers. Terrorists cannot simply march 100 would-be martyrs toward security checkpoints, hoping some might get through. The risks of betrayal and failure are too great. Instead, they study security measures carefully to identify vulnerabilities they can exploit and ways to allay suspicion. Some of these work, but terrorists pay a price in quality control.

Terrorists cannot simply march 100 would-be martyrs toward security checkpoints, hoping some might get through.

SABOTAGE OF AIRLINERS HAS DECLINED, AND SECURITY HAS LED TO LESS-RELIABLE EXPLOSIVE DEVICES

Although the number of terrorist attempts against airliners has declined, sabotage remains a serious threat, as evidenced by continuing plots and attempts to smuggle bombs on board. These include the 2001 failed attempt by the so-called "shoe bomber," the sabotage of two jets in Russia by Chechen terrorists, the 2005 discovery of a bomb that had failed to explode aboard an airliner in Kazakhstan, the 2006 plot to smuggle liquid explosives aboard airliners departing from London's Heathrow Airport, the 2009 sabotage by the "underwear bomber," and the attempt in 2010 to smuggle bombs aboard two courier aircraft heading for the United States. Another terrorist plot to bring down an airliner was foiled by an intelligence operation in 2012. In 2015, terrorists downed a Russian airliner flying from Egypt's Sharm el-Sheikh International Airport, and in 2016, a bomb exploded aboard a Daallo Airlines flight shortly after departing from Mogadishu, Somalia. Terrorist bombs are still getting through security. Four of these 11 incidents were foiled by intelligence operations, but in nine incidents, terrorists were able to smuggle their devices on board.

Three of the devices (2001, 2005, and 2006) malfunctioned, and in the Daallo Airlines attack, the bomb failed to bring down the airliner, and only one passenger—the bomber himself—was killed. Bombs did bring down three airliners (two in 2004 and one in 2015), but the fact that terrorists are forced to build smaller, easier-to-hide devices with exotic ingredients and no metal parts, to make them less detectable, represents a kind of progress for security—the new devices are less reliable, and even if they detonate, they may not bring down the plane. The number of attempts suggest that improved security has discouraged but not deterred sabotage attempts; terrorist groups must now recruit suicide attackers and must have highly skilled bomb-makers whose devices may not always work.

SECURITY HAS PUSHED TERRORISTS AWAY FROM HIGH-PROFILE TRANSPORTATION TARGETS

Terrorist campaigns against surface transportation also illustrate some deterrent effects of security. Early in its terrorist campaign, the IRA bombed railway and subway stations in the heart of London. These were prestige targets. As security measures protecting London Transport increased and members of the public became more vigilant, the terrorists were driven away from high-profile targets to more-remote sites.[58] The terrorists who bombed the London Tube in 2005 avoided detection by carrying their bombs in backpacks rather than leaving them in unattended parcels. Transport staff and passengers had not been instructed to watch for backpacks, and moreover, it had been years since any terrorist attacks had targeted the transportation system.

As security measures protecting London Transport increased and members of the public became more vigilant, the terrorists were driven away from high-profile targets to more-remote sites.

French authorities flooded the Paris Metro and commuter rail stations with soldiers and police following the 1995 detonation of a bomb in an underground station; the blast killed eight people and wounded 80. The terrorists continued their campaign but were obliged to go after other, less-protected targets.[59]

These case studies offer some observations. Insofar as we can tell, in no case did security measures lead to a reduction in the overall volume of terrorism. Terrorist campaigns continued, and globally, terrorism increased. But increased security contributed to terrorists gradually abandoning certain tactics and targets. They no longer tried to kidnap diplomats and other high-ranking officials, and they stopped trying to take over embassies. Over several decades, terrorist attacks on airliners declined. Terrorist saboteurs were able to overcome security measures by building smaller explosive devices that could escape detection, but these devices were less reliable. The terrorists moved away from more-protected surface-transportation targets to more-remote, less-protected locations or resorted to suicide bombings. Again, many other factors also help explain these changes.

Increased security contributed to terrorists gradually abandoning certain tactics and targets.

In general, terrorists broadened their quarry in order to successfully attack softer targets. This required a change in mindset. In terrorist thinking, there were fewer “innocents.” We cannot say whether the rules of engagement changed in response to security measures that drove terrorists away from their initially preferred targets, as a reflection of changes in the ideologies driving terrorist behavior, or because of an inherent process of escalation and brutalization.

The change comes at a cost to society in the form of more wanton killing at places where it is more difficult to prevent—and a cost to terrorist organizations in the form of eliminating any possibility of gaining widespread support, thereby further reducing their already thin chances of permanent political gain. Indiscriminate targeting also provokes debate and divisions in the ranks of the terrorist organizations. Terrorism ultimately descends into self-indulgent violence that is politically irrelevant.

VII. OBSERVATIONS AND CONCLUSIONS

This inquiry, still a work in progress, has distilled a number of observations and conclusions, which may be viewed as findings or even as security maxims. As a body, they illustrate the complexity of the challenges terrorists pose to security planners. These findings can be grouped into four major categories.

TERRORISM POSES A UNIQUE THREAT

The purpose of terrorism is terror: Terrorist actions are meant to inspire fear. Terrorists have limited resources and power—they lack the destructive capability of armies—but that level of capability is not necessary for their purpose. Terrorists have very low resource requirements. They do not require large forces to overwhelm enemy defenses; one determined attacker may suffice. The weapons terrorists need are readily available: small arms, crude explosives, incendiary devices, rudimentary weapons, even knives, axes, or automobiles. These suffice to achieve the terrorists' primary objective, which is the creation of terror.

Terrorists have very low resource requirements.

Terrorists will always have a fundamental advantage over those charged with security: Terrorists can attack anything, anywhere, any time. With finite resources, government cannot protect everything, everywhere, all the time. The consequences of this obvious asymmetry are often ignored.

Terrorist attacks are increasing in volume worldwide, but they remain statistically rare and random. This poses an enormous challenge for determining how much security should be deployed and what to defend.

Terrorists concentrate their attacks on soft targets that lack security. They generally attack where there are no perimeters, no checkpoints, no guards. This is particularly the case outside of conflict zones.

Terrorists can try to overcome security measures by increasing the number of attackers, adding to their arsenal, carrying out suicide attacks, or recruiting inside assistance, but they rarely do so. This suggests that other paths—e.g., attacking softer targets—are easier. When terrorists take advantage of an insider, it is usually because one happens to be already available to them and not because of a targeted campaign to recruit an insider.

Today's violence seems to be headed toward what might be called "pure terrorism"—totally random attacks, devoid of political message or symbolic content, calculated only to kill. This kind of terrorism is extremely difficult to prevent, but it limits what the terrorists may achieve politically. The notion of pure terrorism attracts self-selecting, marginal, and sometimes mentally disturbed individuals who are drawn to the violence itself. And pure terrorism alienates popular support.

The prospects of capture or death do not necessarily have the same effect on terrorists that they do on others engaged in violent activities. Anecdotal accounts suggest that terrorists

whose conversations are being monitored continue with their activities even when they know or suspect that they are under surveillance and are likely to be arrested. Their demonstrated commitment to their cause brings them credit for the group and personal satisfaction as a tactical achievement. At the same time, terrorists often seem to court unnecessary risk in their operations. This does not mean that they are always suicidal, but rather that they demonstrate their commitment and acquire status by deliberately exposing themselves to danger.

ASSESSING THE RISK

Terrorism works: The terrorist threat always appears greater than it actually is. By mounting spectacular acts of violence, terrorists create an atmosphere of fear and alarm—i.e., terror—which causes people to exaggerate the strength of the terrorists and the threat they pose.

Terrorist communications cannot be ignored; the exhortations and instructions they provide to followers may persuade some to act. But their exhortations and threats are not always reliable indications of the level of threat or imminent action. The Internet allows terrorists to constantly threaten, boast, and exhort others to action. These communications constitute a major part of a campaign of terror, which, in turn, will cause people to exaggerate the importance of the terrorists and the threat they pose. We can say only that terrorism includes a high volume of noise and a very small amount of action.

Terrorism includes a high volume of noise and a very small amount of action.

Examining terrorist plots informs us about what the terrorists take into account and worry about in their planning but is of limited help in evaluating security measures. Terrorists continuously think about, plan, and talk about possible attacks. They are not soldiers actively engaged in combat. They have a great deal of downtime, and they spend it conjuring up plans—it is part of being a terrorist. Many of their plots, overheard during surveillance, discovered at terrorist hideouts, or revealed in interrogation, are self-indulgent fantasies.

Security against terrorism is driven not only by what terrorists have done in the past, but also by what society fears they might do in the future. There are tensions here—imagination of what terrorists might do drives public fear, while resource constraints limit security planners to defending against demonstrated attacks. The 9/11 attacks fundamentally altered perceptions of plausibility and prompted fears of attacks of even greater magnitude. Add to this the fact that the perceived consequences of a terrorist attack, more than the probability of its occurrence, determine the perceived risk and, consequently, the demand for security.

Imagination of what terrorists might do drives public fear, while resource constraints limit security planners to defending against demonstrated attacks.

Terrorism does not pose a significant danger to individual citizens. Compared with other forms of violent crime, terrorism poses a statistically minuscule threat to the lives of individuals (the 9/11 attacks notwithstanding). The same disparity holds in countries that have lower

crime rates than the United States but suffer higher levels of terrorist attacks. However, terrorist attacks on targets that appear to be random convey the message that no one is safe. Terrorists' demonstration of reach outweighs the calibration of personal risk.

The primary threat of terrorism is to the community. In addition to causing casualties, terrorist attacks cause damage and economic disruption, create alarm, and oblige governments to devote vast resources to security. Terrorist attacks can prevent peace and provoke wars. These are significant costs.

Terrorism appears to be a condenser of society's broader anxieties. Fear is fueled not merely by the objective measure of risk, but by apprehension about the consequences of immigration, economic uncertainty, and perceived loss of national strength. America's frightened, divided, and angry society is currently its biggest vulnerability. Europe is also experiencing deeply rooted anxieties that the current wave of terrorism is exacerbating.

Public expectations of security are rising even as the general level of violence is falling. Even though the level of terrorist violence in the United States since 9/11 is lower than that experienced during the 1970s and the murder rate is falling, frightened Americans are demanding more security. The reduction in risk to Western nations from war and violent crime has left terrorism as the high ground of threat.

The reduction in risk to Western nations from war and violent crime has left terrorism as the high ground of threat.

Over the long run, public tolerance for any sort of risk appears to have declined. This offers an advantage to terrorists, whose primary purpose is the creation of fear.

Apprehension and intolerance for risk push authorities toward preventive intervention before terrorists launch an attack. New laws in the United States allow prosecution on the basis of intentions alone, thereby allowing authorities to intervene earlier and at the same time permitting more forward-leaning intelligence efforts.

CHALLENGES TO SECURITY

Intelligence plays a critical role in preventing terrorist attacks. While domestic intelligence can be further improved, the success of federal investigators and local police in uncovering and thwarting plots in the United States has been remarkable. However, the numbers here are slippery. Most terrorist plots are interrupted in their early stages, making it difficult to judge whether they would ever have been carried out had the authorities not intervened. We can only say that some would.

Terrorists do not have to penetrate security perimeters to carry out their attacks**.** Public spaces—markets, squares, any crowded venue—serves as a terrorist target. Where the intended target has security, attacks can still occur outside perimeters. If an embassy's grounds are impenetrable, shooting the security guards outside or detonating a bomb across the street or down the block will still make headlines.

The burden of security against terrorist attack is determined more by the magnitude or number of potential targets to be protected than by the actual magnitude of the terrorist threat. A single terrorist incident involving aviation, for example, requires countermeasures at hundreds of commercial airports. Terrorists know and exploit this fact, boasting that their bombs cost only a few thousand dollars, while hundreds of millions must be spent on security.

Security is often and necessarily reactive. It is not difficult for terrorists and "red teams" thinking as terrorists to conjure up more scenarios than those charged with security can possibly protect against. Generally, the threat posed by more-frequently-occurring (and therefore demonstrable) nonpolitical crime drives security more than terrorism does.

Security is not an engineering problem that can be solved once and for all; rather, it is an ongoing contest between security planners and their terrorist adversaries. It must be dynamic. As new security measures are put into place, terrorists will seek ways to evade or obviate them. When the terrorists succeed, further new security measures will be required.

Security is not an engineering problem that can be solved once and for all; rather, it is an ongoing contest between security planners and their terrorist adversaries.

Illusion is an important component of security. What critics dismiss as charade, terrorists take more seriously. Their perceptions of consequences differ.

Despite the fact that terrorism is essentially psychological warfare aimed at the people watching, security strategies rarely include efforts to reduce fear. The current emphasis on resilience refers almost entirely to the physical recovery of vital systems after an attack, not the recovery of society's psychological resistance. As a result, discussions of the threat and consequences of attack contribute to a continuing state of anxiety. Increasing security may not always reduce fear, it may only underscore perceptions of danger. We will return to this critical point.

EVALUATING THE EFFECTS OF SECURITY MEASURES

It is difficult to demonstrate empirically that security measures work. This difficulty results from the unique aspects of terrorism, as opposed to some other forms of economically motivated crime or more-conventional modes of warfare. And it is nearly impossible to measure the effects of individual security measures. Security must be seen as a holistic effort in which the measures facilitate and reinforce each other.

Terrorist successes are not necessarily security failures. And a security success is not always a terrorist failure, as a failed attack may still create alarm and oblige additional security measures to be taken. Nonetheless, further study of actual security failures, not efforts to assign blame, could provide useful insights.

Terrorist successes are not necessarily security failures.

Failure to anticipate and thwart a terrorist attack is considered unacceptable because people believe that those charged with security could (and should) have envisioned such

an attack. While security planners often can and do envision attacks, this expectation puts them in a bind. They cannot get support for security measures against attacks they know might occur, but they are held liable for not implementing such measures if one does occur.

The “rare” quality of terrorist attacks makes it difficult to discern trends except over the very long run. Reductions may occur over decades, but many things are going on at the same time that also may account for them. The resolution of conflicts, the suppression or disappearance of specific terrorist groups, and gradual increases and improvements in security measures make it difficult to quantify the contribution of security measures to a reduction, in the narrower sense.

Physical security measures, by themselves, will not end or reduce terrorism. Ending or even reducing terrorism will require resolving the underlying conflict or suppressing the terrorist groups.

Moreover, although physical security measures rarely catch terrorists, catching them is the wrong criterion of effectiveness.

Security generally works as a deterrent. Terrorists want their operations to succeed, and changing patterns of terrorist attacks over long periods of time, along with anecdotal evidence, suggest that security can deter attacks on certain targets.

Deterrence does not mean that no attack will occur; it means that security measures will displace risk to other, less-protected targets. Avoidance behavior is the most common way terrorists overcome security challenges. This indicates that they are aware of security measures and take them seriously enough to avoid or obviate them, for example, by shifting to other targets. Terrorists have an inherent advantage here. We can observe this effect, but we cannot easily quantify it.

Security measures should aim for a net security benefit. Increasing security in order to merely displace the risk from one target to another, while necessary in special circumstances, offers little net security benefit. This argues against disruptive and costly security efforts to protect public places.

Nevertheless, security measures have demonstrable utility. They can create operational problems for would-be attackers; affect terrorist target selection; reduce terrorist effectiveness; uncover explosive devices; detect weapons; assist authorities in quickly diagnosing and responding to attacks; help to quickly identify and apprehend perpetrators, thereby preventing further planned attacks; and facilitate rapid removal of innocent individuals from harm’s way.

Forcing terrorists to be suicidal reduces their recruiting pool**.** Some terrorists are suicidal—unfazed by the prospect of death—-and this is sometimes offered as evidence of the futility of security as a deterrent. But raising the bar of required commitment is a security achievement, because few people possess that degree of dedication.

Enlisting the public in security demonstrably works. One security measure that can be quantified and that appears to work in the area of surface-transportation security is enlisting staff and the public to call attention to suspicious behavior and objects. Public awareness in the United Kingdom seems to have helped in identifying explosive devices placed by the IRA. According to the MTI database, warnings by staff, on-scene security personnel, and passengers prevented 11 percent of terrorist bombings in Europe. This area merits further research.

Enlisting the public in security demonstrably works.

Cost-benefit analysis is useful in articulating assumptions about the terrorist threat and evaluating security responses, but it cannot be the sole basis for assessing security measures. The readily quantifiable risks of terrorist attacks are too low to justify almost any security measure, while the psychological effects of terrorism are much more difficult to pin down or quantify. Yet it is the reaction to terrorism that poses the greatest threat to a country's political system, economy, and social well-being.

A FINAL COMMENT

To return to an earlier observation, security strategy understandably has focused on risk reduction through prevention, physical protection, rapid response, and mitigation of casualties. These address the *terrorism* component of the threat but ignore the *terror* component. Terrorism and terror are separate domains. We have repeatedly seen that with limited violence, terrorists can achieve disproportionate results in the realm of terror. Indeed, the necessity of arguing for security resources, the responsibility of alerting people to danger, the visible security measures themselves, and the phenomenon of contemporary news-media coverage of terrorist events become accessories in the creation of fear. Although it lies outside the realm of physical security, the possibility of creating a counterterror strategy that draws upon traditional and admired strengths in American society—courage, true grit, coolness under fire, self-reliance, sticking together in the face of danger, helping each other in emergencies—has hardly been explored. Such a strategy does not mean belittling individual fears, but rather building a less-vulnerable mindset.

The possibility of creating a counterterror strategy that draws upon traditional and admired strengths in American society... has hardly been explored.

ABBREVIATIONS AND ACRONYMS

CAPPS	Computer-Assisted Passenger Pre-Screening System
CCTV	Closed-Circuit Television
CPTED	Crime Prevention through Environmental Design
GTD	Global Terrorism Database
IRA	Irish Republican Army
ISIL	Islamic State of Iraq and the Levant
MTI	Mineta Transportation Institute
PNR	Passenger Name Record
START	Study of Terrorism and Responses to Terrorism
TIDE	Terrorist Identities Datamart Environment
TSA	Transportation Security Administration

ENDNOTES

1. I am indebted to Mineta Transportation Institute's Emeritus Executive Director Rod Diridon and its current Executive Director Karen Philbrick for their continued encouragement and support, and to my long-time colleague Bruce R. Butterworth for his assistance in the preparation of this report; to Anita Szafran and Sachi Yagyu for their assistance in locating additional information; to Richard Daddario, David A. Lubarsky, and other reviewers for their thoughtful comments; and to Janet DeLand for her always skillful editing.

2. See About the Author at the end of this report.

3. U.S. Department of Defense, *Dictionary of Military and Associated Terms,* Washington, D.C., 2005.

4. National Consortium for the Study of Terrorism and Responses to Terrorism, *Global Terrorism Database,* University of Maryland, College Park, MD, http://www.start.umd.edu/gtd/

5. Ibid.

6. Ibid.

7. Brian Michael Jenkins and Bruce R. Butterworth, *Database on Attacks on Public Surface Transportation,* San Jose, CA: Mineta Transportation Institute.

8. GTD, op. cit.

9. GTD, op. cit.

10. GTD, op. cit.

11. MTI database, op. cit.

12. The total number of incidents for the decade was divided by 100, and the resulting number was then used as the count to select the incidents.

13. GTD, op. cit.

14. Justin V. Hastings and Ryan J. Chan, Target Hardening and Terrorist Signaling: The Case of Aviation Security, Sydney, Australia: The University of Sydney, 2011.

15. Bee stings kill an average of 53 persons a year in the United States, while spider bites kill an average of 6.5 persons a year—slightly more deaths than have been caused by jihadist terrorists during the past 15 years.

16. U.S. Government, "Homeland Security Funding Analysis in Analytical Perspectives," FY 2017 Federal Budget, Washington, D.C., pp. 347-358.

17. Ibid.

18. Greg Treverton, Justin L. Adams, James Dertouzos, Arindam Dutta, Susan S. Everingham, and Eric V. Larson, "The Costs of Responding to the Terrorist Threats: The U.S. Case," in Philip Keefer and Norman Loayza (eds.), Terrorism, Economic Development, and Political Openness, Cambridge, England: Cambridge University Press, 2008.

19. John Mueller and Mark G. Stewart, "Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security," paper prepared for presentation at the panel, Terror and the Economy: Which Institutions Help Mitigate the Damage? Annual Convention of the Midwest Political Science Association, Chicago, IL, April 1, 2011.

20. These include the 2002 shooting at Los Angeles International Airport, which resulted in the deaths of 2 persons; 2009 shooting in Little Rock, Arkansas, in which one person was killed; the 2009 shooting at Fort Hood, Texas, in which 13 persons died; the 2013 Boston Marathon bombing and subsequent shootout with police, in which 5 persons were killed; the 2015 Chattanooga slayings, which killed 5; the 2015 San Bernardino shootings, which killed 14, the 2016 Orlando shooting, which killed 49 persons. None of the fatality figures include the assailants.

21. Brian Michael Jenkins, personal notes. See also David Inserra, "An Interactive Timeline of Islamist Terror Plots Since 9/11," The Daily Signal, September 10, 2015 (the timeline continues through 2016), http://dailysignal.com/2015/09/10/a-timeline-of-73-islamist-terror-plots-since-911/

22. Mueller and Stewart, op. cit.

23. Brian Michael Jenkins, Andrew Liepman, and Henry H. Willis, Identifying Enemies Among Us: Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing. Santa Monic, CA: The RAND Corporation, 2014; Business Executives for National Security, Domestic Security: Confronting a Changing Threat to Ensure Public Safety and Civil Liberties. Washington, DC: BENS, 2015; for a critical view, see Karen J. Greenberg, Rogue Justice: The Making of the Security State. New York, NY: Crown Publishing Group, 2016.

24. Brian Michael Jenkins and Bruce R. Butterworth, Selective Screening of Rail Passengers, San Jose, CA: Mineta Transportation Institute, 2007, http://transweb.sjsu.edu/MTIportal/research/publications/documents/06-07/pdf/MTI-06-07.pdf; Brian Michael Jenkins, Bruce R. Butterworth, and Larry N. Gersten, Supplement to MTI Study on Selective Passenger Screening in the Mass Transit Environment, San Jose, CA: Mineta Transportation Institute, 2010, http://transweb.sjsu.edu/MTIportal/research/publications/summary/MTI-0905.html

25. Heather Klotz-Young, "Analytics Packed with Power," SDM, July 2014. See also Ayesha Choudhary and Santanu Chaudhury, "Video Analytics Revisited," IET Computer Vision, March 4, 2016; and Dinesh Kumar Saini, Dikshika Ahir, and Amit

Ganatra, “Techniques and Challenges in Building Intelligent Systems: Anomaly Detection in Camera Surveillance,” in S. C. Satapathy and S. Das (eds.), Proceedings of First International Conference on Information and Communications Technology for Intelligent Systems and Technologies, Vol. 2, 2015.

26. John Woodhouse, CCTV and Its Effectiveness in Tackling Crime, Parliament, London, July 1, 2010.

27. Brian Michael Jenkins and Joseph Trella, Carnage Interrupted: An Analysis of Fifteen Terrorist Plots against Public Surface Transportation, San Jose, CA: Mineta Transportation Institute, 2012, http://transweb.sjsu.edu/PDFs/research/2979-analysis-of-terrorist-plots-against-public-surface-transportation.pdf

28. Ibid.

29. Small Arms Survey, Weapons and Markets, “Civilian Inventories,” http://www.smallarmssurvey.org/weapons-and-markets/stockpiles/civilian-inventories.html

30. David A. Fahrenholt and Frederick Kunkle, “U.S. Sees Shortage of Ammunition,” Washington Post, November 3, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/11/02/AR20091102712.html

31. U.S. Congress, Office of Technology Assessment, Taggants in Explosives, Washington, D.C.: U.S. Government Printing Office, April 1980.

32. U.S. Geological Survey, 2014 Minerals Yearbook: Explosives, May 2016, https://minerals.usgs.gov/minerals/pubs/commodity/explosives/myb1-2014-explo.pdf

33. Report of the President’s Commission on Aviation Security and Terrorism, Washington DC: 1990.

34. Office of Technology Assessment, Technology Against Terrorism: The Federal Effort. Washington DC: U.S. Government Printing Office, 1991. http://ota.fas.org/reports/9139.pdf

35. White House Commission on Aviation Safety and Security, Final Report to President Clinton. Washington DC: 1997. https://fas.org/irp/threat/212fin~1.html

36. Jenkins and Trella, op. cit.

37. Brian Michael Jenkins and Jean-Francois Clair, Trains, Concert Halls, Airports, and Restaurants—All Soft Targets: What the Terrorist Campaign in France and Belgium Tells Us About the Future of Jihadist Terrorism in Europe, San Jose, CA: Mineta Transportation Institute, 2016.

38. U.S. Department of State, The Inman Report: Report of the Secretary of State’s Advisory Panel on Overseas Security, Washington, D.C., 1985, http://fas.org/irp/threat/inman/

39. Committee on Research for the Security of Future U.S. Embassy Buildings, The Embassy of the Future, Washington, D.C.: The National Academy Press, 1986.

40. Brian Taylor, Anastasia Loukaitou-Sideris, Robin Liggett, Camille Fink, Martin Wachs, Ellen Cavanagh, Christopher Cherry, and Peter J. Haas, Designing and Operating Secure Transit Systems: Assessing Current Practices in the United States and Europe, San Jose, CA: Mineta Transportation Institute, 2005, http://transweb.sjsu.edu/MTIportal/research/publications/documents/04-05/MTI_04-05.pdf

41. Brian Michael Jenkins, Chris Kozub, Bruce R. Butterworth, Renee Haider, and Jean-Francois Clair, Formulating a Strategy for Securing High-Speed Rail in the United States. San Jose, CA: Mineta Transportation Institute, 2013, http://transweb.sjsu.edu/PDFs/research/1026-securing-US-high-speed-rail.pdf

42. Brian Michael Jenkins and Larry Gersten, Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices. San Jose, CA: Mineta Transportation Institute, 2001, http://transweb.sjsu.edu/MTIportal/research/publications/documents/01-07.pdf

43. Ibid.

44. Brian Michael Jenkins and Bruce R. Butterworth, *Long-Term Trends in Attacks on Public Surface Transportation in Europe and North America*, San Jose, CA: Mineta Transportation Institute, 2016.

45. Ibid.

46. Ibid.

47. Bruce R. Butterworth, Shalom Dolev, and Brian Michael Jenkins, Security Awareness for Public Bus Transportation: Case Studies of Attacks against the Israeli Public Bus System, San Jose, CA: Mineta Transportation Institute, 2012, http://transweb.sjsu.edu/PDFs/research/2978-israeli-bus-public-transportation-attacks.pdf

48. U.S. Government Accountability Office, TSA Should Limit Funding for Behavior Detection Activities, Washington, D.C., November 14, 2013.

49. Michael S. Schmidt and Eric Lichtblau, “Racial Profiling Rife at Airport, U.S. Officers Say,” The New York Times, August 11, 2012, http://www.nytimes.com/2012/08/12/us/racial-profiling-at-boston-airport-officials-say.html?_r=1

50. These include the 2006 car ramming in Chapel Hill, NC; the 2009 shooting in Little Rock, AR; the 2009 shooting at Fort Hood, TX; the 2010 attempt to bomb Times Square in New York; the 2013 bombing in Boston, MA; the 2015 hatchet attack on police in New York City; the 2015 shooting in Garland, TX; the 2015 shooting in Chattanooga, TN; the 2015 stabbings in Merced, CA; the 2015 shooting in San Bernardino, CA; the 2015 shooting in Philadelphia, PA; the stabbings in St. Paul, MN; the 2016 bombing in New York City; and the 2016 automobile and knife attack at

Ohio State University in Columbus, OH. In several of these cases, as well as several others not listed here, there are differences of opinion about whether the perpetrator was mentally ill and claimed allegiance to a terrorist organization merely in order to gain prestige or whether there is sufficient evidence of radicalization to describe him as a terrorist. This list does not include the foreign-instigated attempted attacks on U.S.-bound airliners.

51. This was the conclusion of a RAND study that pointed to the vulnerability created by the lines of people waiting to go through the security check points (Terry L. Schell, Brian G. Chow, and Clifford Grammich, Designing Airports for Security: An Analysis of Proposed Changes at LAX, Santa Monica, CA: RAND Corporation, IP-251, 2003, http://www.rand.org/pubs/issue_papers/IP251.html).

52. Brian Michael Jenkins, "The Response to Every Terrorist Attack Cannot be Another Checkpoint," The Hill, July 1, 2016, http://thehill.com/blogs/pundits-blog/homeland-security/286226-the-response-to-every-terrorist-attack-cannot-be-another

53. Brian Michael Jenkins and Bruce R. Butterworth, By the Numbers: Russia's Terrorists Increasingly Target Transportation, San Jose, CA: Mineta Transportation Institute, 2014.

54. For a sampling of the general discussion of deterrence in the realm of terrorism, see Paul K. Davis and Brian Michael Jenkins, Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda, Santa Monica, CA: RAND Corporation, MR-1619-DARPA, 2002, http://www.rand.org/pubs/monograph_reports/MR1619.html; Brian A. Jackson, Peter Chalk, Kim Cragin, Bruce Newsome, John Parachini, William Rosenau, Erin M. Simpson, Melanie W. Sisson, and Donald Temple, Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies, Santa Monica, CA: RAND Corporation, MG-481-DHS, 2007, http://www.rand.org/pubs/monographs/MG481.html; and Andrew R. Morral and Brian A. Jackson, Understanding the Role of Deterrence in Counterterrorism Strategy, Santa Monica, CA: RAND Corporation, OP-281-RC, 2009, http://www.rand.org/pubs/occasional_papers/OP281.html

55. Brian Michael Jenkins (ed.), Terrorism and Personal Protection, Boston, MA: Butterworth Publishers, 1985. Some of the statistics derive specifically from the chapter by Carol Edler Baumann, "Diplomatic Kidnappings," pp. 23-45.

56. Brian Michael Jenkins, Embassies Under Siege: A Review of 48 Embassy Takeovers, 1971-1980, Santa Monica, CA: RAND Corporation, R-2651-RC, 1981, http://www.rand.org/pubs/reports/R2651.html

57. Brian Michael Jenkins, Aviation Security: After Four Decades, It's Time for a Fundamental Review, Santa Monica, CA: RAND Corporation, OP-390-RC, 2012, http://www.rand.org/pubs/occasional_papers/OP390.html. For an earlier discussion of the effects of aviation security on terrorist behavior, see Paul Wilkinson and Brian M. Jenkins, Aviation Terrorism and Security, London: Frank Cass, Publishers, 1998.

58. Jenkins and Gersten, op. cit.

59. The mid-1990s terrorist campaign in France is described in Brian Michael Jenkins, Bruce R. Butterworth, and Jean-Francois Clair, Off the Rails: The 1995 Attempted Derailing of the French TGV (High Speed Train) and a Quantitative Analysis of 181 Rail Sabotage Events, San Jose, CA: Mineta Transportation Institute, 2010.

BIBLIOGRAPHY

Butterworth, Bruce R., Shalom Dolev, and Brian Michael Jenkins. Security Awareness for Public Bus Transportation: Case Studies of Attacks against the Israeli Public Bus System. San Jose, CA: Mineta Transportation Institute, 2012. http://transweb.sjsu.edu/PDFs/research/2978-israeli-bus-public-transportation-attacks.pdf

Committee on Research for the Security of Future U.S. Embassy Buildings. The Embassy of the Future. Washington, D.C.: The National Academy Press, 1986.

Fahrenholt, David A. and Frederick Kunkle. "U.S. Sees Shortage of Ammunition." Washington Post, November 3, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/11/02/AR20091102712.html

Hastings Justin V. and Ryan J. Chan. Target Hardening and Terrorist Signaling: The Case of Aviation Security. Sydney, Australia: The University of Sydney, 2011. Jenkins, Brian Michael and Bruce R. Butterworth. *Database on Attacks on Public Surface Transportation,* San Jose, CA: Mineta Transportation Institute.

Jenkins, Brian Michael (ed.). Terrorism and Personal Protection. Boston, MA: Butterworth Publishers, 1985. "Diplomatic Kidnappings." pp. 23-45.

Jenkins, Brian Michael. Embassies Under Siege: A Review of 48 Embassy Takeovers, 1971-1980. Santa Monica, CA: RAND Corporation, R-2651-RC, 1981. http://www.rand.org/pubs/reports/R2651.html

Jenkins, Brian Michael. "The Response to Every Terrorist Attack Cannot be Another Checkpoint." The Hill, July 1, 2016. http://thehill.com/blogs/pundits-blog/homeland-security/286226-the-response-to-every-terrorist-attack-cannot-be-another

Jenkins, Brian Michael and Bruce R. Butterworth. By the Numbers: Russia's Terrorists Increasingly Target Transportation. San Jose, CA: Mineta Transportation Institute, 2014.

Jenkins, Brian Michael and Bruce R. Butterworth. *Long-Term Trends in Attacks on Public Surface Transportation in Europe and North America*. San Jose, CA: Mineta Transportation Institute, 2016.

Jenkins, Brian Michael and Bruce R. Butterworth. Selective Screening of Rail Passengers. San Jose, CA: Mineta Transportation Institute, 2007. http://transweb.sjsu.edu/MTIportal/research/publications/documents/06-07/pdf/MTI-06-07.pdf; Jenkins, Brian Michael, Bruce R. Butterworth, and Larry N. Gersten. Supplement to MTI Study on Selective Passenger Screening in the Mass Transit Environment. San Jose, CA: Mineta Transportation Institute, 2010. http://transweb.sjsu.edu/MTIportal/research/publications/summary/MTI-0905.html

Jenkins, Brian Michael and Jean-Francois Clair. Trains, Concert Halls, Airports, and Restaurants—All Soft Targets: What the Terrorist Campaign in France and Belgium Tells Us About the Future of Jihadist Terrorism in Europe. San Jose, CA: Mineta Transportation Institute, 2016.

Jenkins, Brian Michael and Joseph Trella. Carnage Interrupted: An Analysis of Fifteen Terrorist Plots Against Public Surface Transportation. San Jose, CA: Mineta Transportation Institute, 2012. http://transweb.sjsu.edu/PDFs/research/2979-analysis-of-terrorist-plots-against-public-surface-transportation.pdf

Jenkins, Brian Michael and Larry Gersten. Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices. San Jose, CA: Mineta Transportation Institute, 2001, http://transweb.sjsu.edu/MTIportal/research/publications/documents/01-07.pdf

Jenkins, Brian Michael, Andrew Liepman, and Henry H. Willis. Identifying Enemies Among Us: Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing. Santa Monica, CA: The RAND Corporation, 2014; Business Executives for National Security, Domestic Security: Confronting a Changing Threat to Ensure Public Safety and Civil Liberties. Washington, DC: BENS, 2015; for a critical view, see Karen J. Greenberg, Rogue Justice: The Making of the Security State. New York, NY: Crown Publishing Group, 2016.

Jenkins, Brian Michael, Chris Kozub, Bruce R. Butterworth, Renee Haider, and Jean-Francois Clair. Formulating a Strategy for Securing High-Speed Rail in the United States. San Jose, CA: Mineta Transportation Institute, 2013, http://transweb.sjsu.edu/PDFs/research/1026-securing-US-high-speed-rail.pdf

Klotz-Young, Heather. “Analytics Packed with Power.” SDM, July 2014. See also Ayesha Choudhary and Santanu Chaudhury. “Video Analytics Revisited.” IET Computer Vision, March 4, 2016; and Dinesh Kumar Saini, Dikshika Ahir, and Amit Ganatra, “Techniques and Challenges in Building Intelligent Systems: Anomaly Detection in Camera Surveillance.” in S. C. Satapathy and S. Das (eds.). Proceedings of First International Conference on Information and Communications Technology for Intelligent Systems and Technologies, Vol. 2, 2015.

Mueller, John and Mark G. Stewart. “Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security.” Paper prepared for presentation at the panel, Terror and the Economy: Which Institutions Help Mitigate the Damage? Annual Convention of the Midwest Political Science Association. Chicago, IL, April 1, 2011.

Office of Technology Assessment. Technology Against Terrorism: The Federal Effort. Washington DC: U.S. Government Printing Office, 1991. http://ota.fas.org/reports/9139.pdf

Schmidt, Michael S. and Eric Lichtblau. “Racial Profiling Rife at Airport, U.S. Officers Say.” The New York Times. August 11, 2012. http://www.nytimes.com/2012/08/12/us/racial-profiling-at-boston-airport-officials-say.html?_r=1

Small Arms Survey, Weapons and Markets. “Civilian Inventories.” http://www.smallarmssurvey.org/weapons-and-markets/stockpiles/civilian-inventories.html

Taylor, Brian, Anastasia Loukaitou-Sideris, Robin Liggett, Camille Fink, Martin Wachs, Ellen Cavanagh, Christopher Cherry, and Peter J. Haas. Designing and Operating Secure Transit Systems: Assessing Current Practices in the United States and Europe. San Jose, CA: Mineta Transportation Institute, 2005, http://transweb.sjsu.edu/MTIportal/research/publications/documents/04-05/MTI_04-05.pdf

Treverton, Greg, Justin L. Adams, James Dertouzos, Arindam Dutta, Susan S. Everingham, and Eric V. Larson. “The Costs of Responding to the Terrorist Threats: The U.S. Case.” in Philip Keefer and Norman Loayza (eds.). Terrorism, Economic Development, and Political Openness. Cambridge, England: Cambridge University Press, 2008.

U.S. Department of Defense. *Dictionary of Military and Associated Terms.* Washington, D.C., 2005.

U.S. Department of State. The Inman Report: Report of the Secretary of State’s Advisory Panel on Overseas Security. Washington, D.C., 1985. http://fas.org/irp/threat/inman/

U.S. Geological Survey. 2014 Minerals Yearbook: Explosives. May 2016. https://minerals.usgs.gov/minerals/pubs/commodity/explosives/myb1-2014-explo.pdf

U.S. Government Accountability Office. TSA Should Limit Funding for Behavior Detection Activities. Washington, D.C., November 14, 2013.

U.S. Government. “Homeland Security Funding Analysis in Analytical Perspectives.” FY 2017 Federal Budget. Washington, D.C. pp. 347-358.

White House Commission on Aviation Safety and Security. Final Report to President Clinton. Washington DC: 1997. https://fas.org/irp/threat/212fin~1.html

ABOUT THE AUTHOR

BRIAN MICHAEL JENKINS

Brian Michael Jenkins is the director of the Mineta Transportation Institute's National Transportation Center and since 1997 has directed the Institute's continuing research on protecting surface transportation against terrorism and other serious forms of crime.

He received a Bachelor of Arts degree in fine arts and a Masters degree in history, both from UCLA. He also studied at the University of Guanajuato, Mexico, and in the Department of Humanities at the University of San Carlos, Guatemala, where he was a Fulbright Fellow and received a second fellowship from the Organization of American States.

Commissioned in the infantry at the age of 19, Mr. Jenkins became a paratrooper and ultimately a captain in the Green Berets. He is a decorated combat veteran, having served in the Seventh Special Forces Group in the Dominican Republic during the American intervention and later as a member of the Fifth Special Forces Group in Vietnam (1966–1967). He returned to Vietnam on a special assignment in 1968 to serve as a member of the Long Range Planning Task Group; he remained with the Group until the end of 1969, receiving the Department of the Army's highest award for his service. Mr. Jenkins returned to Vietnam on an additional special assignment in 1971.

In 1983, Mr. Jenkins served as an advisor to the Long Commission, convened to examine the circumstances and response to the bombing of the U.S. Marine barracks in Lebanon. In 1984, he assisted the Inman Panel in examining the security of American diplomatic facilities abroad. In 1985–1986, he served as a member of the Committee of the Embassy of the Future, which established new guidelines for the construction of U.S. diplomatic posts. In 1989, Mr. Jenkins served as an advisor to the national commission established to review terrorist threats following the bombing of Pan Am 103. In 1993, he served as a member of the team contracted by the Port Authority of New York & New Jersey to review threats and develop new security measures for the World Trade Center following the bombing in February of that year. In 1996, President Clinton appointed Mr. Jenkins to the White House Commission on Aviation Safety and Security. From 1999 to 2000, he served as an advisor to the National Commission on Terrorism, and since 2000, he has been a member of the U.S. Comptroller General's Advisory Board.

Mr. Jenkins serves as a Senior Advisor to the President of the RAND Corporation. He is a Special Advisor to the International Chamber of Commerce (ICC) and a member of the advisory board of the ICC's investigative arm, the Commercial Crime Services. Over the years, he has served as a consultant to or carried out assignments for a number of government agencies, including the Department of Homeland Security. As part of its international project to create a global strategy to combat terrorism, the Club of Madrid in 2004 appointed Mr. Jenkins to lead an international working group on the role of intelligence. Mr. Jenkins is the author of numerous published research reports, books, and articles on terrorism and security.

PEER REVIEW

San José State University, of the California State University system, and the MTI Board of Trustees have agreed upon a peer review process required for all research published by MTI. The purpose of the review process is to ensure that the results presented are based upon a professionally acceptable research protocol.

Research projects begin with the approval of a scope of work by the sponsoring entities, with in-process reviews by the MTI Research Director and the Research Associated Policy Oversight Committee (RAPOC). Review of the draft research product is conducted by the Research Committee of the Board of Trustees and may include invited critiques from other professionals in the subject field. The review is based on the professional propriety of the research methodology.

MTI FOUNDER

Hon. Norman Y. Mineta

MTI BOARD OF TRUSTEES

Founder, Honorable Norman Mineta (Ex-Officio)
Secretary (ret.), US Department of Transportation
Vice Chair
Hill & Knowlton, Inc.

Honorary Chair, Honorable Bill Shuster (Ex-Officio)
Chair
House Transportation and Infrastructure Committee
United States House of Representatives

Honorary Co-Chair, Honorable Peter DeFazio (Ex-Officio)
Vice Chair
House Transportation and Infrastructure Committee
United States House of Representatives

Chair, Nuria Fernandez (TE 2017)
General Manager and CEO
Valley Transportation Authority

Vice Chair, Grace Crunican (TE 2019)
General Manager
Bay Area Rapid Transit District

Executive Director, Karen Philbrick, Ph.D.
Mineta Transportation Institute
San José State University

Anne Canby (TE 2017)
Director
OneRail Coalition

Donna DeMartino (TE 2018)
General Manager and CEO
San Joaquin Regional Transit District

William Dorey (TE 2017)
Board of Directors
Granite Construction, Inc.

Malcolm Dougherty (Ex-Officio)
Director
California Department of Transportation

Mortimer Downey* (TE 2018)
President
Mort Downey Consulting, LLC

Rose Guilbault (TE 2017)
Board Member
Peninsula Corridor Joint Powers Board (Caltrain)

Ed Hamberger (Ex-Officio)
President/CEO
Association of American Railroads

Steve Heminger* (TE 2018)
Executive Director
Metropolitan Transportation Commission

Diane Woodend Jones (TE 2019)
Principal and Chair of Board
Lea+Elliot, Inc.

Will Kempton (TE 2019)
Executive Director
Transportation California

Art Leahy (TE 2018)
CEO
Metrolink

Jean-Pierre Loubinoux (Ex-Officio)
Director General
International Union of Railways (UIC)

Abbas Mohaddes (TE 2018)
CEO
The Mohaddes Group

Charles W. Moorman IV (Ex-Officio)
CEO
Amtrak

Jeff Morales (TE 2019)
CEO
California High-Speed Rail Authority

Malu Roldan, Ph.D. (Ex-Officio)
Interim Dean
Lucas College and Graduate School of Business
San José State University

Beverley Swaim-Staley (TE 2019)
President
Union Station Redevelopment Corporation

Michael Townes* (TE 2017)
President
Michael S. Townes, LLC

Richard A. White (Ex-Officio)
Interim President and CEO
American Public Transportation Association (APTA)

Bud Wright (Ex-Officio)
Executive Director
American Association of State Highway and Transportation Officials (AASHTO)

Edward Wytkind (Ex-Officio)
President
Transportation Trades Dept., AFL-CIO

(TE) = Term Expiration or Ex-Officio
* = Past Chair, Board of Trustee

Directors

Karen Philbrick, Ph.D.
Executive Director

Peter Haas, Ph.D.
Education Director

Hilary Nixon, Ph.D.
Research and Technology Transfer Director

Asha Weinstein Agrawal, Ph.D.
National Transportation Finance Center

Brian Michael Jenkins
National Transportation Safety and Security Center

Ben Tripousis
National High-Speed Rail Connectivity Center

Research Associates Policy Oversight Committee

Asha Weinstein Agrawal, Ph.D.
Urban and Regional Planning
San José State University

Jan Botha, Ph.D.
Civil & Environmental Engineering
San José State University

Katherine Kao Cushing, Ph.D.
Enviromental Science
San José State University

Dave Czerwinski, Ph.D.
Marketing and Decision Science
San José State University

Frances Edwards, Ph.D.
Political Science
San José State University

Taeho Park, Ph.D.
Organization and Management
San José State University

Diana Wu
Martin Luther King, Jr. Library
San José State University

MINETA
TRANSPORTATION INSTITUTE
MTI

SAN JOSÉ STATE
UNIVERSITY

Funded by U.S. Department of Transportation and California Department of Transportation