This product is part of the RAND Corporation occasional paper series. RAND occasional papers may include an informed perspective on a timely policy issue, a discussion of new research methodologies, essays, a paper presented at a conference, a conference summary, or a summary of work in progress. All RAND occasional papers undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

OCCASIONAL
PAPER

Marrying Prevention and Resiliency

Balancing Approaches to an Uncertain Terrorist Threat

Brian A. Jackson

Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

This Occasional Paper results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by the generosity of RAND's donors and by the fees earned on client-funded research.

Published 2008 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

Created in the wake of the September 11, 2001, terrorist attacks, the Department of Homeland Security came into being with the daunting core mission of taking action to protect the United States from terrorist attack and the simultaneous requirement to continue to perform the numerous other critical functions of all its component agencies. The complexity of the department's mission was further compounded by the fact that it depended not only on the success of the department's component agencies, but also on the efforts of a national homeland security enterprise comprised of organizations at the federal, state, and local levels, both inside and outside government. That there have been challenges in carrying out this endeavor in the years since should surprise no one. However, it has also been the fortunate reality that, whatever those challenges, at the time of this writing, there have been no major terrorist attacks within the United States since 9/11.

Transitions in presidential administrations are traditionally opportunities for the country to examine national policy goals, assess how we as a nation are trying to achieve them, ask whether what we are doing is working, and make adjustments where necessary. For homeland security, the upcoming presidential transition is even more important as it is the first change in administration since the creation of the Department of Homeland Security. To contribute to policy debate during this transition and to inform future homeland security policy development, the RAND Corporation initiated an effort to reexamine key homeland security policy issues and explore new approaches to solving them.

This paper is one of a series of short papers resulting from this effort. The goal was not to comprehensively cover homeland security writ large, but rather to focus on a small set of policy areas, produce essays exploring different approaches to various policy problems, and frame key questions that need to be answered if homeland security policy is to be improved going forward. The results of this effort were diverse, ranging from thought experiments about ways to reframe individual policy problems to more wide-ranging examinations of broader policy regimes. These discussions should be of interest to homeland security policymakers at the federal, state, and local levels and to members of the public interested in homeland security and counterterrorism.

This effort is built on a broad foundation of RAND homeland security research and analysis carried out both before and since the founding of the Department of Homeland Security. Examples of those studies include:

- Brian A. Jackson, Peter Chalk, Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie Sisson, and Donald Temple, *Breaching the Fortress*

Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies, Santa Monica, Calif.: RAND Corporation, MG-481-DHS, 2007.
- Tom LaTourrette, David R. Howell, David E. Mosher, and John MacDonald, *Reducing Terrorism Risk at Shopping Centers: An Analysis of Potential Security Options*, Santa Monica, Calif.: RAND Corporation, TR-401, 2006.
- Henry H. Willis, Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby, *Estimating Terrorism Risk*, Santa Monica, Calif.: RAND Corporation, MG-388-RC, 2005.

The RAND Homeland Security Program

This research was conducted under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment (ISE). The mission of RAND Infrastructure, Safety, and Environment is to improve the development, operation, use, and protection of society's essential physical assets and natural resources and to enhance the related social assets of safety and security of individuals in transit and in their workplaces and communities. Homeland Security Program research supports the Department of Homeland Security and other agencies charged with preventing and mitigating the effects of terrorist activity within U.S. borders. Projects address critical infrastructure protection, emergency management, terrorism risk management, border control, first responders and preparedness, domestic threat assessments, domestic intelligence, and workforce and training. Information about the Homeland Security Program is available online (http://www.rand.org/ise/security/). Inquiries about homeland security research projects should be sent to the following address:

Andrew Morral, Director, Homeland Security Program, ISE
RAND Corporation
1200 South Hayes Street
Arlington, VA 22202-5050
703-413-1100, x5119
Andrew_Morral@rand.org

This Occasional Paper results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by the generosity of RAND's donors and by the fees earned on client-funded research.

Contents

Summary

The uncertain nature of the terrorist threat is a fundamental challenge in the design of counterterrorism policy. For efforts to prevent terrorist attacks before they happen, this uncertainty presents a particular problem: To detect and stop attacks, security organizations need to know how to identify threatening individuals, what type of weapons to look for, and where to be on the lookout in a nation with a multitude of targets attackers might choose among. Though intelligence gathering can reduce threat uncertainty, because of both practical and societal constraints it cannot eliminate it entirely. It is also to terrorist groups' advantage to increase uncertainty by altering their behaviors, tactics, and strategies. This uncertainty complicates decisionmaking about which preventive measures to implement and creates the risk that resources will be expended that—because the threats they are designed to prevent do not materialize as expected—do not produce protective benefits.

These problems have led some to suggest that the country focus on mitigation and resiliency instead of investing in measures designed to prevent attacks. Mitigation and resiliency measures are designed to reduce the impact of a damaging event when it occurs and to make it possible for key infrastructures, economic activities, and other parts of society to rapidly bounce back. While traditional prevention measures buy a chance of preventing all damage from individual attacks by stopping them completely, mitigation and resiliency measures buy a lower, but more certain, payoff: preventing only *some* of the damage from attacks, but doing so predictably across the many different ways in which threats might become manifest. Such measures can also help address risks that have nothing to do with terrorism, such as accidents or natural disasters.

A Hybrid Approach: Consequence Prevention

Instead of seeing an either/or choice between traditional prevention and mitigation or resiliency measures, it is more productive to consider them together in an integrated way—as two complementary elements of a strategy aimed at lessening the *consequences* of successful terrorist attacks. Doing so essentially stretches the concept of prevention beyond the ideal of halting attacks before they happen to also include efforts to limit the human and economic costs of even successful attack operations. The central advantage to viewing prevention in this way is that it broadens the options available to policymakers to include options that are less sensitive to threat uncertainty.

With such a hybrid approach, policymakers would not be constrained to only investing more in intelligence activities to try to eliminate uncertainties or adding layer upon layer of

security in an effort to prevent every attack. Instead, they can assemble combinations of measures that could perform better than either type alone across a wider variety of future threats. This makes it possible to take a portfolio approach to homeland security. In a prevention and mitigation *portfolio*, some measures would reach for the highest payoff of completely preventing attacks, while others would provide a more stable protective return by limiting the damages from any terrorist operation or other event.

For example, in the area of aviation security, traditional preventive measures (e.g., prescreening passengers for air transport) could be combined with measures such as strengthening airframes or placing checked bags and other cargo in containers reinforced to withstand the effects of a bomb detonation. In such a protective portfolio, the mitigation strategies hedge against the chance attackers will be able to get a weapon onto an aircraft and, by doing so, make prevention less of an all-or-nothing proposition.

Similar capabilities-based strategies for hedging uncertain futures have been pursued in other policy arenas, such as defense planning. The Department of Homeland Security already is applying similar approaches in some areas: Capabilities-based planning has been used in response and recovery planning in an effort to build a national portfolio of capabilities that are suitable for a wide range of possible incidents. These strategies might save resources as well—for example, if the costs associated with trying to reduce uncertainty by improving intelligence gathering is high compared with adding additional mitigation measures, spending on the latter might provide more protection per dollar invested.

Assessing Consequence Prevention Strategies

Portfolios that combine different ways to prevent the consequences of terrorist attacks will serve the country better than strategies built from either of these options alone. But how should the results of such an approach be assessed? Determining how much better this approach might be requires examining a variety of such portfolios to explore their strengths and weaknesses across a number of possible futures. To get a full picture, assessments should examine

1. their monetary costs (including direct costs of the measures themselves, their indirect financial costs, and the opportunity costs of using resources one way and not another) to see if such strategies do provide more protection per dollar
2. any intangible costs associated with their impacts on personal privacy, civil liberties, or quality of life, as understanding the full effects of security strategies requires going beyond the costs that are easiest to measure
3. the benefits of the portfolios with respect to preventing terrorism, other potential disruptions, and any other benefits the measures in the portfolio might produce.

Because the goal is developing protective strategies that are not hostage to the uncertain nature of tomorrow's threats, it will be critical to understand how different portfolios perform in different threat and hazard environments, in situations when threats come from unexpected sources, when attackers use varied attack types, and when groups change their strategic and tactical behavior over time. Protective portfolios that perform well across a range of possible futures would be judged less sensitive to threat uncertainty—and therefore more attractive given an uncertain future.

CHAPTER ONE

The Issue

The uncertain nature of the terrorist threat is a fundamental challenge in the design of counterterrorism policy.[1] The differing goals, intentions, preferences, and capabilities of diverse terrorist groups lead to a range of diverse threats. Indeed, most terrorist actions cause little damage and few (if any) casualties, and some groups do not even aspire to more than that. At the other end of the spectrum, groups like al-Qaeda are focused on large-scale destruction.[2] In a large nation with an open society, there are many possible sites that could be targeted by any of these groups. Furthermore, even threats from individual groups change over time: Many terrorist groups have proven to be agile and adaptive, altering their goals and actions in response to changes in their environment and defensive measures put in place to counter them.[3]

In designing homeland security policies, uncertainty about the future threat creates a number of problems.[4] The most significant problems are practical in nature—if we do not know the scale and nature of future threats, deciding how many resources to devote to homeland security efforts and choosing among different security measures is difficult. For protective measures focused on very specialized threats—for example, systems to detect specific chemical or other unconventional weapons—the uncertainty about if or when adversaries will use such weapons means we risk expending effort and funding without ultimately producing a compensatory protective benefit.[5]

---

[1] An additional, higher-level uncertainty is how terrorist-related risks compare with other challenges facing the country, including those from accidental events or natural hazards. There has been substantial policy discussion about the consequences of overly focusing on one source of risk. Although this paper principally addresses challenges associated with the uncertainty surrounding perspective terrorist violence and possible policy responses to that uncertainty, we will also touch somewhat on broader homeland security risk management issues and how different strategies might shape the nation's risk exposure for threats beyond terrorism.

[2] See, for example, the analysis of terrorist attacks on passenger rail systems in Jeremy M. Wilson, Brian A. Jackson, Mel Eisman, Paul Steinberg, and K. Jack Riley, *Securing America's Passenger-Rail Systems*, Santa Monica, Calif.: RAND Corporation, MG-705-NIJ, 2007, pp. 7–16, which shows that although the majority of such attacks produce small consequences, the averages are skewed by a small number of attacks that produce very large numbers of fatalities and injuries.

[3] Brian A. Jackson, Peter Chalk, Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie Sisson, and Donald Temple, *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, Santa Monica, Calif.: RAND Corporation, MG-481-DHS, 2007.

[4] See, for example, discussion in Homeland Security Advisory Council, "Report of the Future of Terrorism Task Force," January 2007.

[5] Drawing on analogous defense planning efforts, uncertainty sets up the possibility for shocks, significant environmental or adversary changes that threaten the effectiveness of current efforts (Paul K. Davis, "Rethinking Defense Planning," John Brademas Center for the Study of Congress, Robert F. Wagner Graduate School of Public Service, New York University, December 2007). In the case of terrorist activity, creating those shocks is a major component of what the terrorist is trying to do.

Methods for Dealing with Uncertainty: Lessons from Defense Planning

Problems with threat uncertainty are not unique to homeland security. Since the end of the Cold War, similar difficulties have been a central theme in broader defense planning and policy analysis. At the end of the last century, with the dominating influence of bilateral U.S.-Soviet conflict removed, defense planners faced a myriad of threats military forces might be expected to respond to, requiring the execution of tasks ranging from conducting major wars to conducting counterterror and counterinsurgency operations to international relief activities. This uncertainty made planning difficult. Efforts to address the planning difficulties caused by the uncertain threat led to the development of analytical techniques such as capabilities-based planning,[6] assumption-based planning,[7] and others. Rather than trying to predict future events and designing defensive capabilities around those predictions, these planning techniques attempt to deal with uncertainty by designing of portfolios of capabilities and testing how the performance of different policy choices might be affected by key uncertainties. With the means to guide allocation of the marginal dollar of national security investment, such approaches also explicitly address the problem that having specific capabilities for all possible threats and contingencies would require unlimited resources.

Dealing with Threat Uncertainty in Homeland Security: We Do It for Response, Can We Do It for Prevention?

Since the founding of the Department of Homeland Security (DHS), capabilities-based planning and similar approaches have been applied to some homeland security policy areas, most notably response and recovery planning. DHS's activities to build the National Preparedness System and implement Homeland Security Presidential Directive–8 (HSPD-8) have laid the foundation for executing this type of planning from the local to the federal levels, including common goals and nomenclature for considering preparedness assets.[8] As in defense planning, their application to homeland security planning helps to address uncertainty about what types of incidents will occur by building capabilities that can be combined in different ways for incidents of varied sizes and requirements.[9] Other approaches based in the fields of risk analy-

---

[6] See, for example, Paul K. Davis, *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation*, Santa Monica, Calif.: RAND Corporation, MR-1513-OSD, 2002.

[7] See, for example, James A. Dewar, *Assumption-Based Planning: A Tool for Reducing Avoidable Surprises*, New York: Cambridge University Press, 2002; and James A. Dewar, Carl H. Builder, William M. Hix, and Morlie Levin, *Assumption-Based Planning: A Planning Tool for Very Uncertain Times*, Santa Monica, Calif.: RAND Corporation, MR-114-A, 1993.

[8] The nature of the national homeland security "enterprise"—where preparedness relies on not just one part of the federal government but on organizations at all levels, including some outside of government (in contrast to the application of capabilities-based planning and other such techniques to national security problems, where planning is more "bounded" within the realms of agencies directly responsible for national defense)—is a major difference between the problems faced by defense and homeland security planners.

[9] DHS's implementation of capabilities-based planning has not been an entirely smooth process: It has been criticized for focusing too heavily on terrorist threats, not being well suited for multiagency planning, lacking clarity in many important respects, and not always translating the results of planning into improvements in national capabilities (see, for example, discussion in Sharon L. Caudle, "Homeland Security Capabilities-Based Planning: Lessons from the Defense Community," *Homeland Security Affairs*, Vol. 1, No. 2, 2005; William O. Jenkins, Jr., "Homeland Security: DHS Improved its Risk-Based Grant Programs' Allocation and Management Methods, But Measuring Programs' Impact on National Capabilities

sis and management have similarly been applied to inform decisions to allocate resources in response to different threats and among different geographical areas.[10]

However, homeland security policy must cover more than just after-incident response and recovery. As laid out in the *National Strategy for Homeland Security*,[11] preventing and disrupting terrorist attacks is a central element of the mission both of DHS and the national homeland security enterprise as a whole.[12] Among security missions, prevention and many disruption activities are particularly sensitive to threat uncertainty and to shortfalls in specific information on perpetrators and their plans. To disrupt a terror cell's planning or an attack in progress, security organizations need to know what to look for, where to position themselves, and who to apprehend, and significant uncertainties can lead to poorly targeted action or to failure.[13] This sensitivity to specific information about the source and nature of the threat makes it difficult to see how—or if—approaches such as capabilities-based planning could inform terrorism *prevention* planning.

These difficulties with "traditional" preventive approaches have led to a focus in some parts of the policy literature on improving the nation's *resiliency* when attacks occur rather than trying to prevent all or even most attacks.[14] The definition of *resilience* differs somewhat in the literature but generally includes measures that make it possible for key infrastructures, economic activities, and other parts of society to rapidly "bounce back" after a disruption, as well as *mitigation* measures to limit potential damage to facilities, supply chains, and other elements of the infrastructure so they can continue to function.[15] These efforts are generally viewed as separate and distinct from efforts intended to prevent attacks entirely and have been presented in some cases as an either/or alternative to preventive approaches[16] or an alternate "overarch-

---

Remains a Challenge," Government Accountability Office, GAO-08-488T, March 11, 2008; Charles R. Wise, "Organizing for Homeland Security after Katrina: Is Adaptive Management What's Missing?" *Public Administration Review*, May/June 2006, pp. 302–318).

[10] See, for example, Henry H. Willis, Tom LaTourrette, Terrence K. Kelly, Scot Hickey, and Samuel Neill, *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*, Santa Monica, Calif.: RAND Corporation, TR-386-DHS, 2007.

[11] Homeland Security Council, *National Strategy for Homeland Security*, October 2007.

[12] In the *National Response Plan*, since replaced by the *National Response Framework*, prevention was defined as "actions taken to avoid an incident or to intervene to stop an incident from occurring . . . to protect lives and property" (DHS, *National Response Plan*, December 2004, p. 53).

[13] As one Coast Guard planner put it in a conversation with the author, prevention efforts are "intelligence intensive"—their value and effectiveness depend on an ongoing stream of timely and good intelligence that reduces or eliminates uncertainty about the nature of the threat.

[14] Notable examples of this literature include Stephen Flynn, *The Edge of Disaster: Rebuilding a Resilient Nation*, New York: Random House, 2007; Yossi Sheffi, *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*, Cambridge, Mass.: MIT Press, 2007; Homeland Security Advisory Council, "Report of the Critical Infrastructure Task Force," January 2006; Robert W. Kelly, "Chain of Perils: Hardening the Global Supply Chain And Strengthening America's Resilience," Reform Institute, March 6, 2008; and Debra van Opstal, "The Resilient Economy: Integrating Competitiveness and Security," Council on Competitiveness, 2007.

[15] Defined in the *National Response Plan* (DHS, 2004, p. 55) as "activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident . . . [that] may be implemented prior to, during, or after an incident."

[16] For example, "The national focus should be on risk management and resilience, not security and protection" (van Opstal, 2007, p. 9).

ing strategy"[17] for addressing terrorism. Since their focus is on the consequences of disruptive events, a central advantage of resiliency and mitigation measures is that their performance is less sensitive to uncertainty in the terrorist threat than traditional prevention.

To deal with the significant uncertainty in the terrorist threat, traditional prevention and mitigation/resilience measures should be considered in a more integrated way, and portfolios of policies should be developed that inform resource allocation choices and the trade-offs between them. The concept of *prevention* should be expanded to include not only the security, intelligence, and law enforcement activities that make up "traditional prevention approaches," but also investments in mitigation and resiliency. By recognizing the distinct contributions these complementary approaches make to preventing the *consequences* of terrorist acts (even if all attacks are not prevented), a strategy of *consequence prevention* should enable better overall "preventive performance" across a range of levels and types of terrorist threats than would be possible viewing them each in isolation. To illustrate the arguments involved, this paper draws examples from aviation security policy and efforts to prevent terrorist attacks in the U.S. air transport system.

[17] For example, "Although it may be argued that current planning for [critical infrastructure protection] encompasses the full risk equation, . . . the focus for action remains on protection through emphasis on reduction or elimination of vulnerabilities. The [Critical Infrastructure Task Force] concluded that making resilience the overarching strategic objective would stimulate synergistic actions that are balanced across all three components of risk" (Homeland Security Advisory Council, 2006, p. 4).

CHAPTER TWO

Background: The Challenges to "Traditional Prevention"

Interrupting terrorist attacks before they occur is attractive for obvious reasons. While effective response and recovery activities can reduce the damage from an attack, successful prevention of attack eliminates the damage entirely. The relative attractiveness of traditional prevention over post-attack action increases with the scale of potential future terrorist attacks. In aviation security, particularly for operations aimed at airliners, the number of potential victims and economic costs from even one successful attack is significant; take, for example, the 2006 plot disrupted in the UK that targeted multiple airliners simultaneously.[1]

But traditional prevention's reliance on information about the nature of the threats is a major challenge. Airport security screeners trying to detect weapons before they get aboard planes need information on what to look for to identify truly threatening items against the noisy background of innocuous materiel individuals take with them as they travel on business or for pleasure. Covert testing by government and other investigators has demonstrated that simulated weapons can often get through security checkpoints, emphasizing the difficulty in ensuring security even when screeners know what they are looking for.[2] As novel threats appear—e.g., the shoe bomb carried by Richard Reid or the liquid explosives that were part of the large-scale plot cited above—new layers of security are put in place and new hazards are added to the list of items being "looked for" at checkpoints in an attempt to exclude them from the system. This reactive approach to the appearance of unexpected threats emphasizes the sensitivity of the detection and prevention effort to uncertainty in the nature of the threat—and undermines public confidence in the system as well.

Attackers also have a number of advantages against traditional preventative efforts that are rooted in threat uncertainty. They can alter their behavior, reducing the value of any threat information that security organizations already have or denying those organizations the knowledge they need to effectively detect and prevent attacks. Individuals attempting to get weapons or other threatening materials through security measures have the options of disguise and deception, seeking to make what they are smuggling look different enough from what is being looked for to slip through or to hide it in other ways.[3] Testing and probing operations can help

---

[1] Described in "Terror Plot Leaves Britain on Highest Alert," CNN.com, August 11, 2006. As of November 12, 2008: http://www.cnn.com/2006/WORLD/europe/08/11/terror.plot/index.html.

[2] See, for example, Gregory D. Kutz and John W. Cooney, "Aviation Security: Vulnerabilities Exposed through Covert Testing of TSA's Passenger Screening Process," Government Accountability Office, GAO-08-48T, November 15, 2007; and Thomas Frank, "Most Fake Bombs Missed by Screeners," *USA Today*, October 17, 2007, p. 1A. Private individuals and journalists have also succeeded in getting a variety of items through security, including prohibited liquids and some types of weapons. See Jeffery Goldberg, "The Things He Carried," *The Atlantic*, November 2008.

[3] Jackson et al., *Breaching the Fortress Wall*, 2007.

attackers determine what they need to know to guide these efforts. Or adversaries can look for ways around the security measures entirely. For example, though a great deal of effort has been focused on passenger screening, concerns remain whether attackers could penetrate airports by entering via the routes taken by non-passengers. Alternatively, rather than attempting to get an explosive device or other weapon into airplane passenger cabins, potential attackers could avoid the heightened attention at the checkpoints by circumventing them entirely by sending it aboard in checked baggage or air cargo.[4]

Defense through traditional preventative efforts is constrained in other ways as well. Adding additional layers of security specific to each new threat is also not a strategy that can be sustained indefinitely. As travelers through today's security checkpoints are well aware, the layers added in response to Richard Reid's actions and the liquid-explosives plot have complicated the screening process. If future threats require additional processes or layers of security, the complexity will only increase. Indeed, if screeners are expected to look for and detect an ever-lengthening list of threats without increasing the time that passengers are detained at security checkpoints, performance against current threats could be hurt. Screening in countries with much tighter security requirements —such as Israel—takes significantly more time to complete.

If it were straightforward to "back off" some security requirements rapidly when they were viewed as no longer justified, the burdens that security measures impose on travelers and the costs they create could be managed dynamically over time. However, making the decision to remove a particular security measure is difficult because adversaries can fairly readily identify what is being screened for and adjust their behavior accordingly—making relaxation of any requirement potentially controversial.[5] The use of spot checking to dynamically create uncertainty in security levels or the characteristics of the screening process could make it possible to step back from the consistent application of all measures to all travelers. But in some cases, such checks would introduce unpredictability for all users of the system (e.g., requiring the removal of shoes at some times but not others), which would create other problems.

When security organizations do not know the source of the threat, security becomes a general requirement imposed on all—e.g., everyone must go through the checkpoints at airports and there are now mandates for examining checked baggage and air cargo requiring 100-percent screening of both.[6] Uncertainty leading to the requirement to impose security in a "broad spectrum" way has an analog in the use of counterterrorism intelligence more broadly. Frequently, counterterrorism intelligence information is not specific warning of attacks at known times and places but rather comes in the form of more-general indicators of an increase in threat or broadened terrorist activity in a specific area or for a given set of potential targets. Without providing guidance about what to look for, such general warnings may only sug-

---

[4] See, for example, discussion in Cathleen A. Berrick, "Transportation Security: Efforts to Strengthen Aviation and Surface Transportation Security Continue to Progress, but More Work Remains," Government Accountability Office, GAO-08-651T, April 15, 2008.

[5] Even the Transportation Security Administration's (TSA's) removal of small scissors and sharp objects from its prohibited items listing was controversial. (Discussed in, Government Accountability Office, "Aviation Security: TSA's Change to Its Prohibited Items List Has Not Resulted in Any Reported Security Incidents, but the Impact of the Change on Screening Operations Is Inconclusive," GAO-07-623R, April 25, 2007.)

[6] See, for example, discussion in Government Accountability Office, "Aviation Security: TSA Oversight of Checked Baggage Screening Procedures Could Be Strengthened," GAO-06-869, July 2006.

gest the need to look more. This is the basis for programs such as the color-coded Homeland Security Advisory System and the use of broader sector-type warnings of potential threats that sought to ramp up or down nonspecific security activities depending on perceived changes in the general threat level. Like mandates for 100-percent screening, the downside of this approach to threat uncertainty is that it produces substantial costs to a variety of actors that can make it difficult to sustain over time. [7]

The main disadvantage of such "broad spectrum" security is its cost. Even short time delays and other costs become substantial as they are added up across the entirety of the traveling public or across all the shipments of cargo back and forth across the country. In addition to the absolute costs involved, there are opportunity costs—the time or resources used to impose a given security check on everyone are time and resources that are not being used to effect other security measures. The fact that such costs can add up quickly means terrorist groups may even trigger security reactions as a tactic for inflicting economic costs.[8]

Strategies for getting away from 100-percent screening—or graduating the intensity of security for different individuals—have their own problems. Attempts to reduce screening burdens through the use of random screening have proven controversial, as observers ridicule instances of "grandmothers" being selected for more-intense screening. Conversely, attempting to target security measures at categories of individuals thought to pose a greater threat holds its own perils.[9] Though such general profiling based on assumptions about likely adversary group members when security organizations lack specific information on threatening individuals may seem intuitive to some, there are a variety of problems that limit its attractiveness. Any general profile about individual characteristics of "likely terrorists" (e.g., their age, ethnicity, or country of origin) is defined by assumptions about the nature of contemporary threats. Any shifts in that threat (e.g., the appearance of new groups with an interest in targeting aviation) could be missed entirely. Similarly, even for current known threat groups, such profiles can create opportunities for attackers. Just as groups can learn what is being "looked for" by probing checkpoints with varied objects in their baggage, they can probe a profile by sending individuals with various characteristics into the system. Once these groups discover which of their members fail to raise an alarm, they know the types of individuals they should be recruiting or using on high-priority missions.[10] Finally, whether or not a profile-driven approach catches any terrorists, it is certain it will ensnare individuals with similar characteristics who have nothing to do with terrorism.

---

[7] See, for example, discussion in Government Accountability Office, "Homeland Security Advisory System," memorandum to the House Select Committee on Homeland Security, GAO-04-453R, February 26, 2004.

[8] See, for example, discussion in Brian A. Jackson, Lloyd Dixon, and Victoria A. Greenfield, *Economically Targeted Terrorism: A Review of the Literature and a Framework for Considering Defensive Approaches*, Santa Monica, Calif.: RAND Corporation, TR-476-CTRMP, 2007.

[9] Here, we are talking about profiling using individual characteristics (choosing specific individuals for more or different screening based on their age, ethnicity, country of origin, and so on) rather than profiling or screening selection based on behavioral characteristics (e.g., individuals exhibiting signs of nervousness as they pass through security or responding to questions about their activities or destination evasively or incorrectly).

[10] See discussion in Jackson et al., *Breaching the Fortress Wall*, 2007.

CHAPTER THREE

Dealing with Threat Uncertainty

Current Approaches

Since uncertainty in the terrorist threat is not a new phenomenon, a number of approaches have been taken to try to address it in traditional prevention efforts. A prominent response has always been to try to gather intelligence to r*educe or eliminate the shortfalls* in what security organizations know about future threats. This is the rationale behind improving and broadening intelligence-collection efforts aimed at filling in knowledge gaps—i.e., by increasing the information available to security organizations about individuals, theoretically making it possible to more effectively identify potentially threatening individuals and reduce uncertainty about who is or is not a terrorist. This was the intent of programs such as the Computer-Assisted Passenger Prescreening System (CAPPS II) and early versions of the Secure Flight program, which were designed to combine information on travelers from a variety of sources to inform an assessment of the risk they posed. Broader intelligence efforts to identify unknown terrorist cells among the general population are focused on achieving this goal for both aviation security and terrorism prevention more generally.

A second response to uncertainty in threats has been attempts to *red-team possible threats and prepare for them now*. This strategy essentially sidesteps uncertainty by preparing for threats ranging from plausible-but-not-yet-realized attack modes to worst-case scenarios in spite of the absence of reliable information on likelihood that they will come to pass.[1] Such activities are frequently part of security planning efforts,[2] sometimes in a response to a view that often arises after successful attacks: Security planners were simply not creative or imaginative enough to anticipate a new or novel threat. The difficulty of this approach is that it is always possible to "conjure up more diabolical scenarios than any security system can protect against."[3] Particularly for higher-end, worst-case attack modes, if every possible scenario creates a demand for its own specialized security measures, attempting to eliminate threat uncertainty via airtight

[1] This is the basic rationale behind the doctrine identified with Vice President Richard Cheney by Ron Suskind: If we believe that there is a 1-percent chance of a threatening possibility (e.g., Pakistani scientists helping al-Qaeda build or develop a nuclear weapon) being true then we must craft our response as if it is 100-percent certain. This approach essentially converts threat *uncertainty* to threat *certainty* by assuming the worst case. Ron Suskind, *The One Percent Doctrine: Deep Inside America's Pursuit of its Enemies Since 9/11*, New York: Simon and Schuster, 2006.

[2] See, for example, Eileen Sullivan, "Appropriators Show Support for DHS' 'Red Team' Scenarios," CQ.com, June 13, 2007 (as of November 12, 2008: http://public.cq.com/docs/hs/hsnews110-000002531281.html); and "Sci-fi Writers Join War on Terror," USAToday.com, May 31, 2007 (as of November 12, 2008: http://www.usatoday.com/tech/science/2007-05-29-deviant-thinkers-security_N.htm)

[3] Brian Michael Jenkins, "Safeguarding the Skies," commentary, *San Diego Union Tribune*, September 30, 2001.

security measures for all possible threats would quickly produce an air-transport system so expensive and inaccessible that it was unusable.

Both of these approaches have serious limits, the most important of which is their various associated costs. Crafting and deploying security measures for every possible terrorist threat quickly becomes cost prohibitive in a country as large as the United States, particularly given the many other demands on national resources. Furthermore, efforts to "cover everything," including all possible upper-end threat scenarios, could also distract attention from higher-probability, less-dramatic scenarios and skew preventive efforts overall. While there are monetary costs associated with strategies focused on intelligence collection, potentially more controversy surrounds the less-tangible costs of these programs. For example, the dramatic and negative reactions to CAPPS II and initial versions of the Secure Flight program were driven by concerns about their effect on personal privacy. These concerns led to the cancellation of CAPPS II and significant modification to Secure Flight. It is also questionable whether enough intelligence could ever be collected to eliminate uncertainty about future threats. Given public sensitivities and the practical difficulties of collecting and analyzing large amounts of information on every traveler, it is likely that a residual of irreducible threat uncertainty will always remain.[4]

An Alternative Approach to Threat Uncertainty: Bringing Together Traditional Prevention and Mitigation Efforts

Given there will likely always be some uncertainty about future terrorist threats, policies that are either less sensitive—or are insensitive—to limits in knowledge would be desirable. This is the basis for the argument for focusing on resiliency rather than traditional prevention—if we don't try to prevent disruptions but instead invest in measures that help us "take the hit" wherever it comes from, then such uncertainties are much less important. However, rather than approach this as an either/or choice between prevention and resiliency, these two strategies can instead be viewed as ingredients for a hybrid preventive strategy: consequence prevention. Traditional prevention efforts undertaken by law enforcement and intelligence organizations may seem different enough from resiliency activities—such as building in blast hardening at potential targets—that thinking about them together might seem strange. But the common denominator is that both are attempting to prevent the casualties and damage that a terrorist attack would cause, albeit in different ways. This is where the concept of *integrated prevention portfolios* comes in: Just as capabilities-based planning made it possible to craft national defense or response policies that can perform acceptably across a range of futures, balancing portfolios of both traditional prevention and resiliency approaches could enable more-stable or even superior "preventive performance" for the country than when they are viewed as unrelated capabilities.

In thinking about terrorism prevention efforts, the usual answer to the question "what are we trying to prevent?" is that we are trying to prevent individual terrorist attacks—to stop each attack an adversary attempts to carry out. When viewed in this manner—where any attack that goes to completion is by definition "not prevented"—improvements to preventive performance becomes largely shackled to the two strategies discussed above: gathering better threat

[4] This is particularly the case given the possibility of strategic behavior by adversaries.

information and deploying tighter and tighter defenses. Security and intelligence measures are intended to give defenders the chance to discover a plot and thwart it; therefore, investments in this arena are aimed at measures that increase that chance.

However, when the answer to the same question is broadened to preventing attackers' ability to kill, injure, or cause other damage, *whether or not their attack is successful*, the field of preventive measures widens and the system's ability to deal with threat uncertainty increases. While one way to prevent the consequences of terrorist attacks is to ensure the operations are not successful by arresting the perpetrators before they can get started, it is not the only way. In this view, an attack could be "partially prevented" if measures were put in place to reduce its impact.

What sorts of security or other policy options might be included in this broader view of prevention? The current literature on resiliency focuses on strategies such as building redundancy into infrastructures and technological systems so single failures affect their functioning less seriously, designing flexibility into organizations' activities and technologies, maintaining agility and adaptability to respond to disruptive events, and setting aside resources and capabilities to rapidly repair the damage when an incident occurs. These strategies largely center on systems and targets that are important for *economic* purposes—infrastructures, private-sector supply chains, manufacturing facilities, and so on—since such approaches grew in part out of thinking about business continuity, private-sector risk management, and the economic consequences of events such as terrorist attacks.[5]

More-inclusive treatments have broadened thinking beyond economic concerns to include more-general societal resiliency, activities such as emergency response and recovery, and other mitigation measures, such as choosing not to build new structures in flood plains, transitioning to less-hazardous industrial processes, and strengthening infrastructure more broadly.[6] To fully cover the range of consequences of terrorist attacks, mitigation approaches intended to limit the casualties from successful attacks also need to be included, and these are often less explicitly covered in the literature on resiliency.[7] Examples of such measures include design choices that reduce the maximum damage or casualties that attacks at potential targets could achieve (e.g., construction of an airport terminal that minimized the size of crowds that gathered in one place)[8] or efforts to prepare the public to react more effectively to particular types of incidents and to harden them to the potential of future attacks.[9]

Unlike traditional prevention efforts, these measures are not focused solely on discovering and completely stopping individual attacks but rather aim to reduce the amount of destruction, casualties, and psychological impact they would cause.

---

5 Sheffi, 2007; Kelly, 2008; van Opstal, 2007; and Jackson et al., *Economically Targeted Terrorism*, 2007.

6 Flynn, 2007; Homeland Security Advisory Council, 2006.

7 However, some measures that are addressed explicitly—e.g., emergency response capabilities—are important when considering constraining the casualties that could be produced by successful terrorist attacks.

8 See, for example, Donald Stevens, Terry L. Schell, Thomas Hamilton, Richard Mesic, Michael Scott Brown, Edward W. Chan, Mel Eisman, Eric V. Larson, Marvin Schaffer, Bruce Newsome, John Gibson, and Elwyn Harris, *Near-Term Options for Improving Security at Los Angeles International Airport*, Santa Monica, Calif.: RAND Corporation, DB-468-1-LAWA, 2004.

9 See, for example, Lynn E. Davis, Tom LaTourrette, D. Mosher, Lois M. Davis, and David R. Howell, *Individual Preparedness and Response to Chemical, Radiological, Nuclear, and Biological Terrorist Attacks*, Santa Monica, Calif.: RAND Corporation, MR-1731-SF, 2003.

Portfolio Approaches to Prevention and Mitigation—Pros and Cons

Why is it useful to think about prevention and mitigation efforts together? Framing prevention in terms of preventing the outcomes of attacks opens up the number of possible approaches to include a wider set of options, many of which are less sensitive to threat uncertainty than "traditional" prevention measure alone. When not constrained to adding additional layers of security or trying to obtain better threat information, policymakers can develop combinations of measures that can perform better against a wide variety of future threats, and can potentially do so at lower overall cost.

Consequence-prevention approaches are less sensitive to uncertainty because, in many cases, they can provide protection even in the absence of knowledge about the nature of an attack, the attackers, or from where the threat is coming. As Debra van Opstal of the Council on Competitiveness observed in an examination of resiliency as an approach to economic consequences of terrorism and other disruption, "There are an infinite number of disruption scenarios, but only a finite number of outcomes."[10] Examples of such strategies for air transport include hardening airframes to make them less sensitive to attacks, changing air handling systems inside planes to reduce the impact of chemical or biological agents released aboard, and using containers for checked bags or other cargo shipped in aircraft holds that would help contain the effects of a bomb detonation. An airframe that is able to better withstand damage from a bomb or that is equipped with cargo containers that can contain the force of blasts does not depend on knowing exactly how an attacker will disguise an explosive device. Similarly, configuring air handling systems so that plane cabins can be flushed quickly (rather than only being able to recirculate air) could reduce the impact of a variety of unconventional attacks, independent of how an attacker managed to get the weapons onto the plane itself.[11] The placement of air marshals on planes represents an example of a more-traditional preventive strategy in which performance does not depend as much on certain threat information. As a late-stage line of defense within actual aircraft, air marshals respond to threats as they manifest—not preventing them completely, but containing their effects as much as possible by stopping them in progress. Unlike defensive measures tuned to specific threat types (e.g., detection technologies tuned to a particular weapon), the marshals can respond to a variety of possible scenarios.[12]

While traditional prevention policies buy a chance of preventing all damage from individual attacks by stopping them completely, the preventive approaches outlined above achieve a more certain but admittedly lower-value payoff: preventing *some* of the damage from attacks. However, they do so predictably across many different ways those threats might become manifest.[13] The lack of sensitivity to where an attack—or any damaging event—comes from means

---

[10] van Opstal, 2007, p. 9.

[11] See, for example, Committee on Assessment of Security Technologies for Transportation, National Research Council, "Defending the U.S. Air Transportation System Against Chemical and Biological Threats," 2006.

[12] This strategy, where security measures can adjust to the expressed threat at the end rather than being specifically designed for a single threat from the outset, is analogous to resiliency strategies discussed for private-sector supply chains where "customization" of a product is held off as long as possible to maintain flexibility and adaptability (see Sheffi, 2007).

[13] Such a strategy is consistent with some approaches to other risks as well—for example, rather than trying to prevent all auto accidents, many measures are put in place to limit the damage when they do occur. It has also been noted that such investments are an "easier sell" to private-sector planners—who own and manage many of the potential targets the country has an interest in protecting—because there will be a more-certain payoff from the investment (van Opstal, 2007, p. 39).

that these measures also can produce benefits even in the absence of an attempted terrorist attack, unlike traditional preventive efforts. More-robust infrastructure systems will work better whether or not the "adversary" involved in an incident is a terrorist group trying to knock out power to an airport or a violent thunderstorm whose effects could produce the same outcome.

Proposing to consider these types of investments alongside traditional prevention thinking does not constitute an argument to give up measures and strategies aimed at preventing individual attacks. Although traditional preventive measures may only "buy" a chance to detect and stop an attack, the opportunity to avoid all the damage from a potential attack does have value. Even in the literature focusing on resilience as a preferred strategy over traditional prevention, preventive measures are often discussed hand-in-hand with measures focused on improving resilience. For example, an analysis by the Homeland Security Advisory Council discussed the need to integrate resilience with protection strategies to reduce the "brittleness" of protection alone. Even assessments focused on the need to improve the resilience of economic systems and infrastructures often include discussion of traditional preventive measures as part of their overall strategy.[14]

However, since the performance of traditional preventive measures will always be uncertain, it would be poor policy to rely on those measures alone. Instead, traditional preventive investments can be traded off against and balanced with resilience measures or mitigation approaches in a hybrid preventive portfolio. Just as the different components of a portfolio of financial investments serve to balance out the overall risk to the investor, adding mitigation measures to prevention efforts can also provide a more stable "security return" over time than would just focusing on traditional prevention approaches. Since what is important for the nation is the *total return* over many years and how much it costs to get that return, both types of measures have parts to play. In addition to making it possible to assemble a more uncertainty-tolerant portfolio of homeland security investments, such a strategy might also save resources—e.g., if the costs associated with improving intelligence gathering are high compared to alternative measures, spending on the alternatives might provide more protection per dollar invested.

Though there is a value to viewing mitigation and consequence-reduction measures as part of an overall terrorism prevention portfolio, one must acknowledge that there are political realities associated with this line of thinking. Though the more predictable benefits these measures provide when different types of attacks happen are their strength, the reality is that these measures function *after* attacks happen.[15] Security approaches that acknowledge that some attacks will likely occur and that the ideal of a society free of terrorism risk is not realistic are not always straightforward and easy to sell to the public. However, as the scale of the financial

---

[14] For example, elements of Stephen Flynn's discussion of intelligence gathering and U.S. Coast Guard preventive efforts (Flynn, 2007); chapters 7 and 8 of Yossi, 2007; and Robert W. Kelly's discussion of container inspection and container protection technologies (Kelly, 2008).

[15] Though the damage-reducing capabilities of these measures only function after attacks happen, mitigation efforts can have some effects on the probability that attacks—or attacks at specific locations or by specific modes—occur by shifting terrorists' choices and decisionmaking. One of the vulnerabilities of purely preventive measures is that groups can see what is being looked for and act to avoid detection. In the case of mitigation measures, it can be harder for groups to fully determine the capabilities and properties of the measure (e.g., the exact details of blast hardening at a target) and to therefore know what they need to do in response. This can push groups to other attack modes, but the more general the mitigation measures, the more possible attack modes the measures devalue for the attacker.

and other costs of measures to prevent terrorist attacks in the United States since 9/11 have become more clear and as the climate of fear that dominated in the immediate aftermath of the attacks has dissipated to some extent, there may be greater opportunities for reframing terrorism prevention to make it more sustainable and effective over the long term.[16] The contrast between the reaction to Secretary of Homeland Security Michael Chertoff's remarks in 2005 that the federal government should focus on preventing larger-scale attacks and leaving others to local agencies (e.g., attacks on the aviation system rather than mass transit)—where he was "grilled" by legislators and some even demanded "an apology" for the statement[17]—and recent remarks by Chairman Bennie Thompson of the House Homeland Security Committee that we should focus on resilience rather than trying to prevent attacks couldn't be more striking.[18]

[16] See, for example, discussion in Homeland Security Advisory Council, "Report of the Future of Terrorism Task Force," January 2007.

[17] Kaitlin Bell, "Chertoff Defends Remarks on Security for Ground Transit," *Boston Globe*, July 15, 2005.

[18] Rep. Bennie G. Thompson, Chairman, House Homeland Security Committee, "The Resilient Homeland—Broadening the Homeland Security Strategy," statement, May 6, 2008 (as of November 12, 2008: http://homeland.house.gov/SiteDocuments/20080506102135-80363.pdf)

CHAPTER FOUR

How Might the Impact of This Approach Be Evaluated?

Though conceptually attractive, operationalizing the proposal outlined in this discussion would require a number of steps. The heart of the concept is a trade-off between investments that are not generally balanced against each other—e.g., intelligence- or information-analysis programs used by TSA to prescreen passengers versus things such as hardened containers to carry cargo in the belly of aircraft. Assessing the consequences—both intended and unintended—of such a change in policy requires further analysis.

The heart of this type of assessment is the development of systematic ways to evaluate the value of different portfolios of preventive measures and the determination of how to make a judgment that one portfolio—e.g., one containing a mix of traditional preventive with mitigation or resilience measures—is superior to another having a different composition. These judgments could be based on monetary costs (including the direct costs of the measures themselves, their indirect financial costs, and the opportunity cost of using resources one way instead of another); any intangible costs associated with their effect on personal privacy, civil liberties, or quality of life; or the benefits of the portfolios might produce, both with respect to terrorism and other potential disruptions and more broadly.[1]

Though there are challenges in making judgments about all of these factors, assessing the counterterrorism benefits of security or other measures is particularly difficult. RAND has used probabilistic models developed by the insurance industry to analyze the distribution of different types of terrorism risk across the country,[2] but for the type of portfolio assessment considered here such analysis would have to be married with models of how different types of preventive measures would reduce that risk so the relative benefits of different portfolios could be estimated.[3] These insurance-focused models quantify benefits as avoided costs—casualties that are not caused, damage that does not occur, or other costs from things like business interruption that do not arise—because prevention was effective.

In thinking about the country as a whole, other metrics might be appropriate to consider as well. For example, since 9/11, the fact that another major attack has not occurred has been a common metric cited in public discourse.[4] Irrespective of their utility as an overall assess-

[1] See Jackson et al., 2007 for discussion.

[2] Tom LaTourrette and Henry H. Willis, "Using Probabilistic Terrorism Risk Modeling for Regulatory Benefit-Cost Analysis: Application to the Western Hemisphere Travel Initiative Implemented in the Land Environment," Santa Monica, Calif.: RAND Corporation, WR-487-IEC, May 2007.

[3] An example of a simplified approach to this type of analysis is available in Wilson et al., 2007.

[4] Whether or not it is appropriate to make the causative assumption that the lack of attacks is a result of current approaches to counterterrorism and homeland security is not important for this discussion—for our purposes it suffices to simply

ment of counterterrorism efforts, mitigation or resilience-heavy portfolios would by definition trade a potential increase in the incidence of attacks against a reduced scale of the damage they produce because mitigation measures seek to reduce damages rather than stop attacks entirely. To the extent that preventing attacks (whatever their scale) is considered a separate value from reducing total damages, the number of attacks that might occur given different portfolios could be a relevant measure of comparison.

With a set of outcome measures guiding judgments regarding the value of different policy portfolios, this approach to terrorism prevention could be tested by comparing the performance of portfolios dominated by more-traditional preventive measures against those built using a wider variety of policy options. Given uncertainty about future threats, this can be done by constructing alternative futures or using scenario analysis to test how portfolios will perform under different sets of assumptions. Across the range of different factors cited above, preventive portfolios that performed well across a range of possible futures would be judged less sensitive to threat uncertainty—and therefore more attractive given an unknowable future—than those whose performance varied significantly from scenario to scenario.

An actual scenario analysis would incorporate a wide range of ways that the future might vary and, given that the benefits of different preventive and mitigation/resiliency measures vary across different hazards, would address variation not just in terrorism but in other potential disruptions and other events as well. A complete future-scenario analysis is beyond the scope of paper, but the following are some of the relevant ways the future terrorist threat might vary that would need to be considered.

Overall Level of Terrorist Threat. Although we make investments in terrorism prevention with the assumption that they will produce benefits by reducing terrorism risk, what if few—or even no—terrorist attacks actually occur? Since 9/11, the nation has been fortunate that there have been no major terrorist attacks in the homeland. Though counterterrorism efforts presumably have something to do with this, the possibility exists that the future could be less threatening that we expect either due to the success of international counterterrorism efforts or other unforeseen shifts in terrorist behavior and activity. In an unexpectedly low-threat future, portfolio performance would hinge not on the traditional preventive benefits of the portfolio but on any additional, nonterrorism benefits that the measures produce. Because consequence prevention measures can have much broader benefits than traditional counterterrorism surveillance and prevention—e.g., building resilience into systems protecting against natural as well as man-made threats—under these circumstances portfolio performance might be dominated by the nontraditional components within it.

Source of the Threat. Though the current concern is al-Qaeda, future terrorist threats could come from very different sources. For example, with environmental problems gaining increasing prominence, organizations that have focused on that issue in the past might broaden their activities or shift to more lethal operations.[5] The source of the threat could shape the

recognize that a count of major or other attacks is a politically relevant metric for assessing different portfolios of policy options.

[5] Groups such the Earth Liberation Front and Animal Liberation Front have generally restricted their operations in scale and have sought to cause monetary damage but not human or animal casualties. A shift by such groups—or by splinter groups—to operations that cause larger-scale damage or kill significant numbers of people would represent a major change in direction and would presumably require a catalyst, such as obvious and major environmental events originating from climate change.

attractiveness of more traditional prevention approaches versus approaches that are less sensitive to threat uncertainty. If threats come from the generally expected sources, intelligence gathering and analysis that is designed around policymakers' current judgments as to where threats are coming from now will have the best chance to perform well.

On the other hand, if future threats come from unexpected sources, traditional preventive approaches may be "looking in the wrong direction" when attacks materialize. For example, if groups with environmental agendas seek to attack the air transport system, their operatives are unlikely to resemble those of al-Qaeda–associated groups, and security technologies and procedures optimized for the current threat may or may not identify them. There is also no reason to assume that the attack modes of these groups will resemble those expected from al-Qaeda today and so may or may not be the types of weapons security screeners in airports are looking for.[6] In such a situation, the performance of consequence-mitigation strategies would become more important for the performance of the overall portfolio.

Mix of Attack Types. The performance of different portfolios of preventive measures could diverge depending on the types and variation in attacks that occur in the future. Preventive portfolios that include measures aimed at mitigating the effects of explosives attacks at key targets—one of the most common terrorist attack modes—would perform poorly if the majority of future attacks are unconventional in nature. The relative effectiveness of traditional prevention approaches versus mitigation approaches could also vary considerably among attack modes. For example, attacks with nuclear devices will not be straightforward to address using most mitigation- or resiliency-based approaches (at least not within realistic cost constraints), and so more traditional prevention would likely be the superior approach in these instances. On the other hand, biological attacks that might be very difficult to prevent might be very sensitive to mitigation strategies.[7]

Variation in Strategic Behavior by Adversaries. Though it is broadly recognized that some terrorist organizations change their behavior, tactics, and target choices in response to the decisions made by security organizations, not all do so equally well. The nature and extent of such changes in behavior represent an additional type of threat uncertainty that security planners must contend with. Different preventive portfolios could be more or less sensitive to such shifts; for example, some general mitigation measures that are not target specific, such as emergency response capabilities, are useful across a wide range of contingencies. Adversary choices that seek to magnify the costs of their attacks (e.g., intentionally trying to cause security organizations to ramp up their vigilance or increase security in ways that produce direct or indirect economic costs) are another type of such strategic behavior. Mitigation measures that are "put in place once" (e.g., blast hardening or changes in design of airframes) are immune from such attacker attempts where many traditional prevention approaches are not.

Though this discussion has only sketched an alternative futures analysis in the broadest of strokes, other analytical approaches and methods exist that make it possible to evaluate policies across a much wider range of possible futures and assess their performance in many different ways. A variety of such methods have been developed and used at RAND for prob-

---

[6] For example, in a recent tactical analysis of a variety of terrorist groups, environmental organizations were unique in using incendiary weapons much more than most terrorist groups. See Brian A. Jackson and David R. Frelinger, "Rifling Through the Terrorists' Arsenal: Exploring Groups' Weapon Choices and Technology Strategies," *Studies in Conflict and Terrorism*, Vol. 31, No. 7, 2008, pp. 583–604.

[7] The author gratefully acknowledges Paul Stockton for suggesting this example.

lems ranging from national defense planning to natural resource management. Most apply different approaches to e*xploratory analysis* to examine the performance of different combinations of policies or choices in complex areas where significant uncertainty makes it difficult, if not impossible, to identify and select one optimal way forward. Such approaches identify many variables that could differentiate possible futures—in contrast to the handful of factors described in the previous paragraphs—and how their variation across ranges of uncertainty could affect the value of particular policies.[8]

The goal of such techniques is to select policies that, in combination and within relevant cost and other constraints, will perform reasonably over a range of possible futures. The most elaborate of such analyses use computer models to examine hundreds or thousands of possible future scenarios and assesses the performance of different policy combinations. Policy portfolios that perform well across many futures are less sensitive to uncertainty about how the future will unfold compared to portfolios whose success relies on the validity of specific assumptions. Such approaches similarly can make it possible to ask higher-resolution questions about the implications of policy changes such as those discussed here—for example, how they might alter the distribution of resources or security across the country,[9] the cross-agency effects of the shift (because not all traditional prevention or even consequence prevention activities are housed within DHS), and the distribution of costs among the public and private sector.[10]

---

[8] See, for example, discussion of a variety of RAND applications of these approaches, including the specific tools named Robust Decisionmaking (RDM) and the RAND Portfolio Analysis Tool (PAT) in Robert J. Lempert, Steven W. Popper, Steven C. Bankes, *Shaping the Next One Hundred Years: New Methods for Quantitative, Long-Term Policy Analysis*, Santa Monica, Calif.: RAND Corporation, MR-1626-RPC, 2003; James A. Dewar, *Assumption-Based Planning: A Tool for Reducing Avoidable Surprises*, New York: Cambridge University Press, 2002; Paul K. Davis, Russell D. Shaver, Justin Beck., *Portfolio-Analysis Methods for Assessing Capability Options*, Santa Monica, Calif.: RAND Corporation, MG-662-OSD,2008; Paul K. Davis, Jonathan Kulick, and Michael Egner, *Implications of Modern Decision Science for Military Decision-Support Systems*, Santa Monica, Calif.: RAND Corporation, MG-260-AF, 2005.

[9] For example, in air transport, some mitigation measures would protect very broadly (e.g., reinforced cargo containers that flow through the entire system across the country), while others would not (e.g., specific improvements at high-volume airports.) Such differences could create new equity issues in the distribution of both resources and security.

[10] For example, some mitigation measures in air transport could significantly increase the weight of planes or cargo, which, in an era of expensive jet fuel and airline efforts to reduce the weight of planes whenever they can, would create significant new costs for the private sector. Environmental arguments could also be made about such policies.