OCCASIONAL
PAPER

Emerging Threats and Security Planning

How Should We Decide What Hypothetical Threats to Worry About?

Brian A. Jackson, David R. Frelinger

RAND Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

OCCASIONAL
PAPER

Emerging Threats and Security Planning

How Should We Decide What Hypothetical Threats to Worry About?

Brian A. Jackson, David R. Frelinger

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.

Library of Congress Cataloging-in-Publication Data

Jackson, Brian A., 1972-
Emerging threats and security planning : how should we decide what hypothetical threats to worry about? / Brian A. Jackson, David R. Frelinger.
p. cm.
Includes bibliographical references.
ISBN 978-0-8330-4731-1 (pbk. : alk. paper)
1. National security—United States—Planning. 2. Terrorism—United States—Prevention. 3. United States—Defenses—Planning. 4. Strategic planning—United States. I. Frelinger, Dave. II. Title.

UA23.J25 2009
355'.033573—dc22

2009018478

Published 2009 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 nation 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 level, 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.

This paper is one of a series of short papers resulting from a research effort initiated by the RAND Corporation during the transition in presidential administrations in 2008–2009. As the first change in administration since the creation of the Department of Homeland Security, this period represented an opportunity to reexamine and revisit the goals of homeland security policy and assess how we as a nation are trying to achieve them, ask whether what we are doing is working, and make adjustments where necessary. The goal of RAND's research effort 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 W. 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.

Although the ideas and frameworks described in this paper have been developed over several years of research for the Department of Homeland Security, the National Institute of Justice, the Defense Threat Reduction Agency, the Office of the Secretary of Defense, and other sponsors, the views expressed herein are not necessarily those of RAND or of any of its research sponsors. The authors would also like to acknowledge the contribution of the two reviewers of the manuscript, Dennis Pluchinsky and Brian Michael Jenkins, whose comments were very helpful in improving the paper. Its remaining shortcomings are the sole responsibility of the authors.

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

Preface iii
Tables vii
Summary ix

Emerging Threats and Security Planning: How Should We Decide What Hypothetical Threats to Worry About? 1
The Variety of Emerging Threats Challenging Security Planning 2
Framing a Middle-Ground Approach to Addressing Emerging Threats 4
Identifying Niche Threats 7
Prioritizing Emerging Threat Scenarios 10
Conclusions: Security Planning for the Niche and the Novel 14

References 17

Tables

1. Characteristics of Attacks Related to Operational Risk..... 11
2. Risks Related to Technical Issues During an Attack..... 12

Summary

Concerns about how terrorists might attack in the future are central to the design of security efforts to protect both individual targets and the nation overall. Attacks that differ from those current defenses are designed to address may have a greater chance of success, larger effect, or inspire broader fear among the public. In thinking about emerging threats, security planners are confronted by a panoply of possible future scenarios coming from sources ranging from the terrorists themselves—from either their public statements or intelligence collected on their deliberations—to red-team brainstorming efforts to explore ways adversaries might attack in the future.

What should security planners do with these lists of hypothetical attacks, attacks which can vary from new ways of using standard weapons to the application of unusual technologies like lasers to stage attacks? Should they attempt to defend against all of them, producing a constant strain on security resources and potentially disrupting current security efforts aimed at addressing proven threats? Or should they ignore all of them and focus on general-purpose security approaches, thereby reducing the chances of being distracted or misdirected by threats of unusual hypothetical attacks but potentially sacrificing the opportunity to discover currently unrecognized vulnerabilities? Given adversaries that seek not only to harm but also to disrupt their target societies, both of these courses of action have potential negative consequences: Not responding to threats may give terrorists an advantage in attack, but overreacting to new and novel threats may achieve the very disruption the terrorists seek. As a result, the prudent path clearly lies somewhere between these extremes, meaning that planners need systematic and defensible ways to decide which hypothetical or unusual threats to worry about and how to prioritize among them.

For assessing emerging and/or novel threats and deciding whether—or how much—they should concern security planners, we suggest a commonsensical approach framed by asking two questions:

1. ***Are some of the novel threats "niche threats" that should be addressed within existing security efforts?*** Some novel threats—even plausible ones—represent such a small niche within the total threat posed by terrorists or other adversaries that it is very difficult to make the argument that putting specific security measures in place to address them is justified. The judgment to classify a potential threat scenario as a niche threat might be driven by an assessment that the attack mode provides only modest advantage compared to currently available tactics, its characteristics make it unlikely to be broadly adopted by attackers, the vulnerability the threat seeks to exploit is not so great to provide them major advantage, the consequences if attackers do execute the scenario are

modest, or a combination of such factors. This translates to a judgment that the threat does not merit disproportionate worry and instead can be reasonably treated as a "lesser included case" within a larger part of the overall terrorist threat.

2. ***Which of the remaining threats are attackers most likely to be able to execute successfully and should therefore be of greater concern for security planners?*** Having eliminated some emerging threats as niche threats, security planners will most likely be left with a list of residual threats they must consider. Of those, given finite security resources, decisions will have to be made regarding which to prioritize. In our past work, as a stand-in for formal or quantitative analysis, we assessed novel attack scenarios based on how difficult or risky they would be for a potential attacker. All other things being equal (e.g., for threats with comparable potential consequences), an emerging threat scenario that is easier for an attacker to carry out successfully should be of greater concern to security planners than one that is more difficult to execute. This approach uses a measure of the number and types of ways a terrorist attack scenario could break down when attackers are trying to carry it out as a proxy measure for some elements of the risk associated with the scenario. Use of common measures for weaknesses in terrorist plots makes it possible to compare disparate terrorist scenarios.

This two-stage approach strives to retain as many of the advantages as possible of both extremes of response suggested above. If threats can reasonably be considered niche threats, they can be prudently addressed in the context of existing security efforts. Doing so helps to maintain the stability and effectiveness of those efforts and to limit the disruptiveness of terrorists suggesting new ways they might attack. If threats are unusual enough, suggest significant new vulnerabilities, or their probability or consequences means they cannot be considered lesser included cases within other threats, prioritizing them based on their ease of execution provides a guide for which threats merit the greatest concern and most security attention. This preserves the opportunity to learn from new threats yet prevents security planners from being pulled in many directions simultaneously by attempting to respond to every threat at once.

Emerging Threats and Security Planning: How Should We Decide What Hypothetical Threats to Worry About?

> *We sometimes focus on tactics that may be exotic and esoteric . . . but for most terrorists, they're looking for what works.*[1]

In building counterterrorism and homeland security capability, security planners at all levels face a variety of tradeoffs. Past attacks demonstrate that terrorist groups can attack targets many ways, and even among these proven threats, planners must weigh the costs and benefits of different security measures and allocate finite resources among them. For example, planners know that terrorists have staged attacks on commercial aviation with man-portable surface-to-air missiles, but they still must make the difficult decision as to whether the benefits of ways the nation could address this threat are sufficient to justify their cost. To protect both individual targets and the nation as a whole, planners must build portfolios of security activities to deal with known and predictable threats—such as terrorists using guns and bombs—while also hedging against low-probability but potentially high-consequence attack modes. Because effective protection from terrorism must be sustained 24 hours a day, 7 days a week, planners must build cost-effective, sustainable security capabilities that can be justified and maintained in the face of other competing demands on resources and other risks.

Novel and unusual threats pose a challenge to such security planning. When emerging threats "pop onto the radar screen" of security planners—either as vulnerabilities that have just been discovered or attack modes terrorists have been overheard considering—they must decide whether the new threat requires change to status quo security efforts. Some novel threats clearly do merit concern: If the hypothetical attack does indeed exploit a previously unrecognized vulnerability, then it may significantly increase the chance of a successful terrorist attack. However, other emerging threats do not: If they are sufficiently low probability or would result in modest consequences, disrupting current security efforts to address the new threat may create more problems than it solves. Although there is clearly a value in adjusting and improving security plans over time, it is also important to not create unnecessary disruption. But making the decision that a novel threat does not merit a response carries its own risks for security planners, in the form of professional or political consequences if a similar attack subsequently occurs. As a result, planners need an approach to considering the range of conventional and unconventional, plausible and fanciful ways terrorists might attack that gives them the ability to make prudent and defensible judgments as to which threats are merely distractions that

[1] FBI Chief Intelligence Officer Donald Van Duyn, testimony before the Senate Committee on Homeland Security and Governmental Affairs, January 8, 2009.

would consume scarce time and attention that should be spent on more-critical threats, which in turn will help them make the difficult tradeoffs inherent in counterterrorism and homeland security decisionmaking. Based on the results of a variety of RAND research efforts, this paper presents what we believe is a systematic and commonsense approach for doing so.

The Variety of Emerging Threats Challenging Security Planning

Since the terrorist attacks of September 11, 2001, focused national attention on how terrorist operations could take advantage of previously unrecognized vulnerabilities in security or defensive measures, there has been significant focus in security analysis and planning on identifying and seeking to close other potential vulnerabilities. One part of this vulnerability-driven approach has been an effort to identify potential new attack modes or terrorist scenarios.

The nation's terrorist adversaries have been remarkably helpful and forthcoming in the search for these potential emerging threats. Enabled by the World Wide Web and the desire of a broader community of people—particularly among individuals sympathetic to al-Qaeda and jihadist-inspired terrorism—to feel like they are participants in a larger terrorist struggle, vast numbers of hypothetical terrorist plots flow through Internet chat rooms and message boards. Examples include speculation about what infrastructures might be vulnerable to what kinds of attack, how various esoteric chemicals might be used to injure or kill, and even how electrical generators might be used to create lightning to use as a weapon.[2] Emphasizing that even jihadist sympathizers explicitly engage in threat brainstorming, a 2009 contribution to an Internet posting board specifically asked its members to offer up potential scenarios for al-Qaeda targeting of U.S. corporations ("Jihadists Offer Hypothetical Scenarios, Targets for Attack," 2009). Whether the authors of the threats are truly putting them forward for consideration as actual attacks, are trying to mislead, or are simply engaging in the terrorist equivalent of creative writing is not clear, but the potential for such scenarios to result in scattering the nation's resources and scrambling security plans is real whatever their intent or motivation.

The open nature of this discourse has made it easy for us to see, and this pool of many possible attacks is supplemented by information gathered by intelligence agencies through other means. Though many (or most) of the operations detected during such activities are, in the words of John Pistole, Deputy Director of the Federal Bureau of Investigation, more "aspirational than operational" ("Alberto Gonzales Holds a News Conference on the Miami Terrorist Cell Arrests," 2006), if nothing else, they provide a constant stream of novel potential attacks to challenge security planners. Reports of possible attack scenarios also sometimes appear in the press when they become of sufficient concern that collected information is shared outside intelligence and security organizations. Over the last few years, examples of such threats have included concern about specific ways terrorists might conceal explosives, the use of remote-con-

[2] See, for example, translations of such postings provided by the SITE Intelligence Group's subscription-based Internet monitoring service. Examples of such postings include: "Suggestion to ISI for Using Electricity as a Weapon," al-Ekhlaas posting, translation dated June 13, 2008; "Jihadist Suggests to Poison Europeans' Water," al-Ekhlaas posting, translation dated August 9, 2008; "Suggestion for Dirty Bomb in East and West," al-Ekhlaas posting, translation dated July 22, 2008; "Jihadist Seeks Advice to Poison Police in Iraq," al-Ekhlaas posting, translation dated May 6, 2008.

trol toys in attack scenarios on airplanes (Transportation Security Administration, 2007), and heightened concern about attacks on specific targets as a result of intelligence information.[3]

Beyond the myriad of threats—many fanciful, some more practical—that terrorists produce on their own, security planners' concern about the possibilities of unidentified, lurking vulnerabilities has led to a number of efforts to dream up new ways terrorists might attack. These efforts often seek to identify novel or emerging threats by cross-pollinating the creativity of terrorism analysts with ideas from technology experts, novelists, and other creative personalities. They have included government efforts such as the Department of Homeland Security Information Analysis and Infrastructure Protection Division's Analytic Red Cell program (Mintz, 2004) or the Defense Threat Reduction Agency's *Thwarting an Evil Genius* research effort (Advanced Systems and Concepts Office, undated), threat brainstorming within larger study or planning efforts,[4] interactions between Hollywood writers and creative talent and security analysts or planners to jointly dream up new types of attacks (Calvo, 2002), the work of individual analysts or researchers examining single threats of potential concern (e.g., Baird, 2006; Deshpande, 2009; Bunker, 2008; Lockwood, 2008; see also discussion in McGill, 2008), and even unsolicited contributions by groups such as science fiction authors voluntarily acting as outside sources of creativity (Hall, 2007; Magnuson, 2008; Barrie, 2008).

The fruits of these brainstorming activities are frequently not disclosed outside of government out of concern of giving "bad guys good ideas." However, examples from some are available publicly. Scenarios examined in the Department of Homeland Security's red cell program reportedly included whether terrorists could take advantage of a hurricane in staging an attack and specific ways high-profile events might be targeted (Mintz, 2004). The science fiction writers group put forward that they thought there is "a strong possibility that Al Qaeda or someone else will set off five to ten nukes simultaneously around the country" (Andrews, 2007). Other analyses have looked at whether specific weapon systems could be used to attack particular targets of concern, such as the use of high-tech mortars in assassination operations (Bonomo et al., 2007) or bringing heat-seeking missiles to bear on high-temperature components of electric power grids (Committee on Science and Technology for Countering Terrorism, 2002, p. 181). Individual analysts have contributed scenarios ranging from the idea that "a small terrorist cell could very easily develop an insect-based weapon"[5] for transmitting disease to the use of laser weapons (Bunker, 2008; Elias, 2005) to "pyro-terrorism"—the use of large fires to cause terror (Baird, 2006; Deshpande, 2009).

These sorts of efforts to inject imagination into security planning are reinforced each time a successful, apparently unforeseen attack occurs; where the occurance of the attack leads to the conclusion that past efforts to foresee new risks have involved insufficient—or the wrong kinds of—creativity.[6]

---

[3] For example, threats to the New York City and Washington, D.C., transit systems in 2008 (Hsu and Johnson, 2008).

[4] For example, examination of a wider variety of ways terrorists might attack different parts of the national infrastructure within the National Academies' post–9/11 study examining how science and technology could contribute to securing the nation (Committee on Science and Technology for Countering Terrorism, 2002).

[5] Jeffery Lockwood, quoted in Adams, 2009.

[6] For example, the National Commission on the Terrorist Attacks on the United States put failures of imagination alongside failures in policy, capabilities, and management in its explanation of why the 9/11 attacks succeeded (National Commission on the Terrorist Attacks on the United States, 2004, pp. 339–360). Since then, concerns about failures of imagination in security planning became a common theme when considering homeland security and terrorism preparedness.

Framing a Middle-Ground Approach to Addressing Emerging Threats

Between institutionalized efforts to produce novel threat scenarios and the ideas that constantly emerge from the terrorists themselves, security planners are constantly confronted with a wide variety of hypothetical future threats and potential vulnerabilities. So how should they respond? Which of the nearly infinite number of possible scenarios should planners worry about? The advantages and disadvantages of different approaches can be illustrated by the extremes of a spectrum of possible responses.

At one end of the spectrum of possibilities, a *hyper-vigilant approach* would see each possible threat as requiring appropriate preventive steps and planning for response should such an attack occur. Although planning a response to every possible imagined attack scenario would immunize policymakers from the criticism that "more could have been done" in the event an attack does occur, forcing planners to respond to the threat-du-jour is disruptive (and potentially discrediting) to existing security efforts, which may be effective for the vast majority of likely terrorist threats. Adding new protections can be costly, and if additional resources are not added to implement new prevention and response plans, security for current threats could suffer. As security resources are stretched to try to eliminate the possibility of terrorists flying model airplanes or breeding mosquitoes, the possibility that their performance will suffer against more-usual threats—terrorists toting guns or planting time bombs (see, for example, Lal and Jackson, 2006)—is very real.[7] It is also the case that driving to respond to every new threat risks focusing on scenarios that may or may not be that attractive to real attackers—just because a new attack option is available does not mean it will automatically be viewed as superior to other ways of attacking by terrorist groups, nor that they will be able to execute it successfully even if they make the attempt.[8] In some cases, there can be particular pressures aimed at selected scenarios out of the universe of possible future attacks. Whether out of unique concern about them or other reasons, some threats can attract individual or organization advocates that push for closing specific vulnerabilities. Such pressures are less disruptive than attempts to address every possible threat, but they can impact security plans and place undo stress on limited resources.

Of even greater concern, attempting to respond to all possible threats and responding to threats in an ad hoc manner both play into the hands of the very terrorist groups security measures are intended to defeat. For terrorists that are trying to inflict economic damage on a country, generating a stream of new threats leaders feel obligated to spend money to protect against is a very effective, low-cost and low-risk way to achieve their goals. Whipsawing a society with a constant stream of new reasons for concern creates anxiety and fear, as well as potentially distracting from threats of more-immediate consequence. Effective terrorists (and other adversaries) understand the extra punch that new and unusual threats can have, and

---

[7] An additional challenge is created because frequently, the more unusual the threat, the more specific the apparent required countermeasure. For example, to completely address the possibility that terrorists could use model airplanes to deliver small bombs from the air, defenses that can detect and stop such planes might seem necessary (e.g., Bolkcom, 2006; Miasnikov, 2005). However, such defenses may protect only against this exact type of attack and not be applicable to other types of threats.

[8] For example, while many of the threat scenarios crafted in brainstorming efforts or identified in terrorist Web chatter are very complex and intricate plots, in practice, most terrorists try to keep operations tactically simple, generally rely on tried-and-true weapons for staging attacks, and typically plan and execute their operations on a limited budget.

consequently have every incentive to raise the specter of new weapons or tactics or to cast the things they are doing now as new, even when they are not.

The opposite end of the spectrum would be a *laissez-faire strategy* intentionally worrying less about the possibility that terrorists might find new ways to attack than that the uncertainty about how they will do so makes responding to hypothetical threats unproductive.[9] Rather than ensuring that security measures address each emerging threat that arises, this planning strategy focuses resources on security and preparedness measures that are not sensitive (or are less sensitive) to where the future threat is coming from, and so will be useful whatever unusual emerging threat scenario comes to pass.[10] The key advantages of this approach are that (1) it constrains security expenditures, (2) the investments that are made are more likely to pay off since they are valuable in a wider range of circumstances, and (3) it limits the ability of adversaries to disrupt security plans or cause economic damages by telegraphing new and unusual ways they might attack. But it has the disadvantages that (1) by not paying attention to possible novel threats security planners sacrifice the opportunity to identify unanticipated vulnerabilities that could be inexpensively eliminated and (2) it produces the real political risk that, after an attack, planners will be open to charges that not enough was done to respond to known threats. It also neglects the reality that even general and versatile security and preparedness measures (e.g., public health and medical surge capacity for responding to bioterrorism, whatever the disease) include specific elements that depend on the nature of the threat (e.g., fielding a comprehensive medical surveillance program, crafting medical response plans, and developing vaccines or antibiotics for specific diseases of concern).

A prudent response to future threats obviously falls somewhere between the straw men sitting at the extreme ends of this spectrum and would reflect differences in the nature of different threats, the targets security planners are concerned about protecting, and other factors. But such an intermediate approach requires a systematic and defensible means of deciding which threats to worry about and how much planners should worry about them. Ideally, the national approach to addressing possible future threats should strive to get as many of the advantages of both ends of the spectrum—responding prudently to threats that do reveal new vulnerabilities, but not allowing doing so to threaten the effectiveness and sustainability of existing security efforts by forcing planners to spend disproportionate time focusing on unlikely terrorist scenarios. Analysts could use techniques such as risk analysis or cost/benefit analysis to assess different threats and use their results as a common denominator to determine how much we should worry about different possible attacks and the advisability of different

---

[9] A security strategy at this end of the spectrum would also not expend resources to generate more possible threats through brainstorming activities. Questioning the value of generating these sorts of emerging threats scenarios is the message of what might be called a "counter-brainstorming" effort held by security expert Bruce Schneier. On his blog, he has staged an annual challenge to his readers to come up with "movie plot threat scenarios." Movie plot threats were defined in the inaugural contest as "fears [of terrorist attacks] based on very specific attack scenarios" and in later years as scenarios hinging on the violent use of otherwise innocuous everyday objects to attack airliners (potentially leading to passengers being prohibited from possessing them) and threats specifically designed to sell security or safety products. Each year the contest has attracted hundreds of entries—which Schneier has used to make the point that such scenarios, even possible or even plausible ones, are of comparatively little value for security planning (see Schneier, 2006 and 2007).

[10] For example, in his writings, Bruce Schneier advocates for focusing investments on intelligence/investigation and emergency response (see, Schneier, 2008, pp. 15–19). In past RAND work, we have framed this somewhat differently as requiring tradeoffs between investments that require certainty about future threats to be effective (e.g., traditional prevention approaches) with those that do not (e.g., robustness, resilience, and recovery from incidents) (see Jackson et al., 2008).

possible responses to them.[11] However, for most emerging threats, the information needed for a rigorous risk analysis will not be available. As a result, the security planner confronted with many possible—and difficult to compare—hypothetical attack scenarios needs more approximate ways to decide which are of most concern and suggest ways to deal with them.

This paper draws on a body of previous RAND research projects to suggest an approach to assessing novel threats. It is informed by thinking about the relative risk of different possible attack scenarios, but implements the planning concepts developed in that body of work in a decision-logic process rather than using formal or quantitative analysis. At the heart of this process lie two questions to ask about novel threats:

Are some of the novel threats "niche threats" that should be addressed within existing security efforts?

The first step of our decision-logic captures the advantage of responding to unusual threats via standard security approaches or minor modifications of those approaches. Some novel threats—even plausible ones—represent such a small niche within the total threat posed by terrorists or other adversaries that it is very difficult to make the argument that putting specific security measures in place to address them is justified. The judgment to classify a potential threat scenario as a niche threat might be driven by an assessment that the attack mode provides only modest advantage compared to currently available tactics, its characteristics make it unlikely to be broadly adopted by attackers, the vulnerability the threat seeks to exploit is not so great to provide them major advantage, the consequences if attackers do execute the scenario are modest, or a combination of such factors. This translates to a judgment that the threat does not merit disproportionate worry and instead can be reasonably treated as a "lesser included case" within a larger part of the overall terrorist threat.

Which of the remaining threats are attackers most likely to be able to execute successfully and should therefore be of greater concern for security planners?

Having eliminated some emerging threats as niche threats, security planners will most likely be left with a list of residual threats they must consider. Of those, given finite security resources, decisions will have to be made regarding which to prioritize. In our past work, as a stand-in for formal or quantitative analysis, we assessed novel attack scenarios based on how difficult or risky they would be for a potential attacker. All other things being equal (e.g., for scenarios with comparable potential consequences), an emerging threat scenario that is easier for an attacker to carry out successfully should be of greater concern to security planners than one that is more

[11] Risk is a measure that combines information about threat (the probability an adversary will actually stage a particular attack), vulnerability (the probability that the attack would produce damage if it was staged), and the nature of those potential consequences. *Threat* results from the presence of an adversary group that intends to carry out a particular attack and has the weapons and capability to do so. Therefore, the threat can be viewed as the probability that any scenario will occur in a given period; this probability is produced by evaluating each adversary group's intentions and capabilities. *Vulnerability* is a result of (1) the specific security and protective measures surrounding a target and (2) whether those measures address a particular attack scenario. In the case of attack scenarios that are well addressed by current security planning, vulnerability may be quite low. For novel attacks, however, current security approaches may not be relevant. Vulnerability can also be thought of as the probability that an attack scenario will produce damage rather than be disrupted or defeated by security measures. *Consequences* are the type and scale of damage that a successful attack can produce. In most risk analyses of terrorist incidents, consequences are estimated by the number of people that could be killed or injured in a particular attack or by the economic costs that could result.

difficult to execute.[12] This approach uses a measure of the number and types of ways a terrorist attack scenario could break down when attackers are trying to carry it out as a proxy measure for some elements of the risk associated with the scenario. Use of common measures for weaknesses in terrorist plots makes it possible to compare disparate terrorist scenarios.

The logical analysis underpinning our means of addressing each of these questions is described in more detail in the following sections.

Identifying Niche Threats

When a novel threat comes to light—whether through captured intelligence, open source analysis, or threat brainstorming—it is tempting to focus only on what is new about it compared to threats that are already known and addressed by security planners. For example, upon hearing that terrorist groups have been experimenting with the use of remote-controlled planes and unmanned aerial vehicles (UAVs, e.g., Gormley, 2005; Karmon, 2005; Jane's Terrorism and Insurgency Centre, 2003; "Troops Seize Rebels' Explosive Planes," 2002; "Al-Qaeda Online: Understanding Jihadist Internet Infrastructure," 2006), the fact that such technologies could provide them with the ability to deliver bombs or other weapons from the air on any of many targets stands out is not surprising (Miasnikov, 2005; Gormley, 2003; Verton, 2005). This specific threat was the topic of a recent RAND analysis examining how security planners might deal with terrorist interest in these systems. In creating the framework for this analysis, RAND developed a process for assessing whether a threat requires specialized responses or whether it could be addressed as a lesser included case within larger portions of the threat space (Jackson et al., 2008).[13]

A priori, the idea that terrorists could use UAVs to attack targets from the air seems like a challenge to security planning that might demand a major response—and a threat that would be difficult to treat as a subset of other threats. Measures such as concrete barriers and posted security guards have been put in place around some potential targets such as public buildings or infrastructure targets to keep vehicle bombs from entering, and a remote-controlled airplane may at first blush appear to be a way that terrorists could simply fly right over these defenses. Obvious responses to this concern might include fortifications to keep small planes from being able to fly into key targets, radars powerful enough to detect very small aerial objects, or even air-defense systems at important locations to shoot such "flying bombs" out of the sky. All such measures are aimed at the difference between this threat and others (the fact that the weapon is being delivered from the air) and seek to directly neutralize that difference.

But by focusing on an individual novel threat independent from all other threats and on those characteristics that set it apart from other threats, planners are only considering part of the picture. Terrorists will not think about UAVs in isolation and security planners should not do so either. For the terrorist planning an attack, UAVs are one possible attack mode among many, and their use will be driven by how they compare to other options. Our analysis of the emerging UAV threat therefore included what we called a "red analysis of alternatives" in

[12] This approach represents a movement from vulnerability-based analysis to a more threat- and capabilities-driven assessment process.

[13] Our analysis investigated the potential use of both UAVs and cruise missiles in asymmetric attack scenarios in the U.S. homeland, but for the sake of simplicity, in this discussion we will examine only UAVs.

which we explicitly catalogued the many different ways terrorists could attack targets in addition to using UAVs so that we could systematically compare the advantages and disadvantages to terrorists of this attack mode.

For example, to solve the operational problem posed by defenses around targets, terrorists could use a UAV to deliver a bomb, but they could also choose another less-well-defended target, chose an attack mode that could penetrate those defenses (e.g., a person carrying a bomb into the defended building), design an attack that can overwhelm the defense (e.g., a vehicle bomb powerful enough to be successful in spite of the barriers or guards), or even choose another way to attack from the air (e.g., using the mortars or rockets that many terrorist groups already routinely use) (Jackson et al., 2007). Many of the alternative ways of solving this operational problem are weapons and tactics that are much more familiar to terrorists and would not require them to acquire and learn to operate a UAV or remote-controlled plane.[14]

In addition, by identifying this attack mode as only one choice among many, our analysis of terrorists' alternatives clearly demonstrated that UAVs have additional downsides for attackers compared to other ways they could stage an attack that would have similar consequences. Using a UAV adds risk to attack operations that would simply not otherwise be involved. For example, using a bomb-laden remote-controlled plane in an attack is very sensitive to the wind and weather—with a non-zero chance of an embarrassing outcome such as the weapon ending up stuck in a tree. A person can deliver the same bomb more predictably, rain or shine. Furthermore, most UAV systems also constrain the size of the weapon that can be used in an attack, limiting the scale of causalities and damage an attacker could hope to produce. Small UAVs and many remote-controlled planes have payload capacities well below even the weight of explosives typically carried by suicide bombers; large UAV payloads are on the order of car bombs and from one-third to one-thirtieth the size of truck bombs (Jackson et al., 2008, p. 20). Some or all of these issues would likely make the UAV attack mode less attractive to terrorists, in spite of the UAV's possible advantages.

As a result, while it is certainly possible that some terrorists will pursue UAVs and even use them in attacks, there appear to be no factors that would lead to their broad adoption by many terrorist groups. Furthermore, even if they were, it does not appear that the consequences of such attacks would be significant for most potential terrorist targets. In truth, if a terrorist

---

[14] In our analysis, we examined a number of other operational problems where it appeared that UAVs might be of particular utility to attack planners. They were:

- If border security measures made it more difficult for attackers to enter the country, some long-range UAVs could allow attacks to be staged from outside the country.
- If groups had only a small number of members but wanted to stage many simultaneous attacks, UAVs launched from a single point to many targets could make that possible.
- If groups were concerned about being apprehended after staging an attack (e.g., by being identified by witnesses at the target or through examination of closed-circuit television footage from private and government systems that captured their identity when they entered the target to stage the attack), UAVs could allow them to attack from afar and make it easier to stage a long-term terrorist campaign.
- If groups wanted to disseminate an unconventional weapon (e.g., chemical or biological agent) over a target, a UAV could make that easier to do.

Just as was the case for the use of UAVs to avoid perimeter security, other "tried-and-true" solutions to these problems are available to potential attackers. In addition, in some cases (e.g., concern about border security excluding terrorists from the country), it is not clear how much of a challenge these problems are to relevant terrorist groups. Finally, in the case of unconventional weapons, terrorist possession of such weapons is a far more important concern than whether they use a UAV or some other way of staging such an attack (Jackson et al., 2008).

was choosing between a common weapon (such as an emplaced or vehicle-borne bomb) and a UAV carrying an explosive payload to strike a target, security planners may actually *prefer* he or she use the UAV since doing so would limit the potential damage and casualties from the attack in many cases where other means of striking the target are feasible.

This combination of likely modest use by a few groups and modest consequences from that use leads to the conclusion that UAVs should be largely viewed as simply one more means among many of delivering a moderately-sized bomb to a target rather than as a novel threat in their own right. Though they can provide attackers some advantages in some situations, they are neither game-changing nor impactful enough that they represent more than a small slice of the overall threat faced by a modern nation from terrorism. Therefore, and because they are a small subset of a broader threat—in this case explosives use—UAVs are a niche threat.

Given their niche status, security planning should then focus on how to address UAVs within broader counterterrorism efforts rather than consider specialized defenses designed to address them in particular. For example, major and costly changes in security measures, such as the deployment of localized air defenses, would be unwarranted for all but the most exceptional targets because the scale of the threat would make such expensive changes nearly impossible to justify. In our analysis, the core of a prudent response to the threat of UAVs was broader investments in measures such as proliferation control and monitoring efforts and broader policing, all of which could produce benefits with respect to both UAVs and other threats. This core was supplemented with measures specific to the threat of UAVs *only* when those efforts were low cost, such as the technical study of UAV systems that would aid in forensic investigation should an attack using the technology occur.

Though our discussion focused on UAVs as a niche within the larger threat of terrorist use of explosives, other examples of such threats are readily available. The concern about terrorists using remote-controlled toys in attacks discussed above is an analogous threat, representing just one of many different ways an explosive device could be initiated and providing limited advantages over those other ways. Concern about terrorists detonating multiple nuclear weapons simultaneously (Andrews, 2007) falls within the general threat of nuclear terrorism, though at the highest end of the spectrum. Of the more exotic threats discussed previously, the potential terrorist use of disease-carrying insects in attacks (Lockwood, 2008) can also be viewed as a niche threat, though in this case a niche either within the threat of bioterrorism or within the even broader risk of insect-borne disease, both natural and man-made.

The process of assessing emerging attack scenarios to determine if they can reasonably be treated as niche threats has several advantages from the perspective of security planning. Forcing comparisons with the many ways that terrorist groups have available to stage attacks now—rather than only focusing on those characteristics that make a new threat new—forces the objective assessment of how much of an advantage an attacker would really achieve by pursuing a novel attack. If that advantage is modest—i.e., the scope of the potential consequences compared to other attacks is similar or smaller and the operational characteristics are not substantially superior—then there will be less of an incentive for terrorists to pursue that attack mode in the first place. Consequently, there is less reason for security planners to attempt to defend against the threat. Defaulting to addressing such threats within existing security measures is then a prudent way to hedge against the risk that some attackers might attempt the attack, but it also limits disruption to existing security efforts and reduces the chance of diverting security resources to a low-probability threat.

Prioritizing Emerging Threat Scenarios

But what about attack scenarios that can't be treated as niches of more general threats? Terrorists using lasers as weapons (Bunker, 2008) or building devices to produce synthetic lightning[15] are unusual enough scenarios that they are difficult to treat as lesser included cases of other, more-common threats. But just because a threat is new does not mean security planners must worry about it. Given finite resources, security planners need approaches to help decide how much they should consider even genuinely novel threats and of those, which they should tackle first and how much should be spent doing so.

This problem is further complicated by the need to compare threats that are very different to make decisions regarding the allocation of limited security dollars. It is not easy to compare threats as diverse as laser attacks and synthetic lighting, much less compare them to more pedestrian terrorist tactics such as bombings or armed attack. This difficulty in comparing threats can be a further pressure toward putting security measures in place for each of them individually, thereby sidestepping the need to compare them. But security planning undertaken in this manner can quickly get expensive. Common denominators are needed to make it possible to weigh different threat scenarios and make judgments about which merit customized security measures, which should be addressed by general measures like response and recovery, and which can most likely be ignored.

So how might security planners compare such disparate threats? One obvious element is some estimate of potential consequences of an attack, where higher potential consequences—many casualties or a high degree of damage—would make an emerging threat of greater concern. But focusing on consequences alone provides only a partial picture, ignoring the other two components of risk—threat and vulnerability—that drive the likelihood of a terrorist attempting an attack via that mode and whether the potential targets would be damaged should such an attack be staged. However, for most emerging or hypothetical threats, a rigorous risk assessment is impossible because, almost by definition, planners cannot know the probability that such attacks will be attempted or what targets (vulnerable or not) they might be carried out against. To sidestep this problem, we use an approach that compares different terrorist operations by ranking them based on the *estimated likelihood terrorist attackers will be able to carry them out successfully*. This process includes asking questions about how easy or hard it would be for attackers to execute a specific attack scenario given its requirements and characteristics (an aspect of threat) and the potential effects of security measures on their likelihood of success (an aspect of vulnerability). To do so, we drill down into the details of each emerging threat scenario to uncover the practical elements of what would actually be involved in staging an attack using a novel weapon or tactic.

At a detailed level, some attack modes are simply more likely to encounter problems than others. For example, terrorists relying on improvised weapons (e.g., homemade mortars) would—in general—be more likely to encounter problems than groups using proven commercial weapons (e.g., mortars produced by an arms manufacturer). Similarly, very complicated operations (e.g., attacks dependant upon multiple events occurring in tight succession) would be more likely to break down than more-simple attack plans. Sometimes terrorists can hedge against these risks; sometimes they cannot. In our work, we identified six general characteris-

[15] SITE Intelligence Group translation of jihadist internet posting on the al Ekhlaas forum, "Suggestion to ISI for Using Electricity as a Weapon," translation dated June 13, 2008.

tics that affected the likelihood of a terrorist operation running into problems or failing entirely.[16] Those characteristics are summarized in Table 1.

If emerging threat scenarios can be systematically assessed to identify how they differ based on these characteristics, then even very different types of operations can be compared, since common failure modes and the factors that shape the likelihood of those failure modes causing the operation to go awry provide a common basis for comparison.[17] Combined with an understanding of the potential consequences of different operations, it can also provide the basis for prioritization of threat scenarios: All other things being equal, novel threat scenarios that are robust and more likely to succeed should be of greater concern than intricate and complicated operations that, although they might be attempted by attackers, are much more likely to break down as a result of their operational requirements, skill demands, and other factors.

Actually executing this approach to assess specific emerging threat scenarios requires a process to systematically measure them against the six factors in Table 1. To do so, we devel-

Table 1
Characteristics of Attacks Related to Operational Risk

Characteristic	Operational Risk
Operational Complexity and Difficulty	
Technology characteristics	Operations that rely on tried-and-true technologies involve fewer risks than those that rely on improvised or very complex technologies.
Skill requirements	Operations that rely only on general knowledge that attackers can develop on their own are less demanding than those that require very specialized skills that might require training to develop.
Requirements for simultaneous or tightly sequential actions	Operations that require that actions occur either at the same time or in a specific order over a short period to be successful are riskier than those that do not.
Potential Operational Breakdowns	
Elements that make operation detectable by security organizations or law enforcement	Operations that require overtly hostile action or are inherently detectable are more likely to fail than more-clandestine activities.
Potential protective measures to prevent or disrupt the attack	Operations that are sensitive to the security and protective measures around a target are more likely to fail than those that are insensitive to them.
Reliance on events outside the attackers' control	Operations that rely on events (e.g., the exact time a target will arrive at a specific location) that are not under the attackers' control involve more risk than those that do not.

[16] In designing small-unit operations, military organizations have established processes for thinking through factors that could threaten operational success. One example of these processes is the Mission, Enemy, Terrain, Troops and Equipment, and Time Available analysis method used by the U.S. military to perform operational risk analysis. The general characteristics that we identified to assess possible terrorist scenarios roughly parallel the elements of that structure, which include assessment of how equipment (technology), opposing actors (from the perspective of a terrorist, the security forces), operational design (including complexity) and other unexpected factors could increase the chance of a negative outcome in a military operation. See, for example, U.S. Army, 1998.

[17] This general approach is derived from such risk analysis methods as fault-tree analysis and failure-mode-and-effects analysis, but our approach is much more conceptual and qualitative than is usual in these formal methods (see, for example, Haimes, 2004, Chapter 13, for a discussion of these techniques. An example of the use of fault trees for analyses relating to terrorism is available in Shooman, 2006).

oped high-medium-low ranking scales for each of the characteristics and measures for the complexity of different attack operations to qualitatively score risks for different scenarios.[18] Table 2 presents an example of a scale for rating a scenario's technical risk. Similar scales can be constructed for the other characteristics and the ways that different failure modes could occur in different phases of an operation, including preparing for the attack (e.g., manufacturing weapons), approaching and engaging the target, carrying out the attack itself, and (if applicable) disengaging and escaping.

In laying out these sorts of scales for ranking different operations, we do not mean to imply that the terrorist attackers are choosing operations or making their own decisions based on this sort of systematic process. While it is not inconceivable that some might—and there is certainly evidence that attackers take factors such as risk or their level of confidence in their weapons into account as they think about operations—it is unlikely that any group would use as structured a process as the one outlined here. That said, even if no terrorist makes decisions in this manner, it is still useful for security planners to break down potential terrorist operations systematically because the factors they identify will contribute to whether or not an attempted operation is likely to succeed no matter how approximate or non-systematic a process the attackers went through to reach the conclusion that staging the attack was a good idea.

Returning to the two novel threat scenarios used as examples previously—terrorist use of lasers and their building a machine to generate artificial lightning—it is easy to see how this sort of qualitative ranking process can be used to differentiate among very different hypothetical attacks. Assuming that an attacker would buy an industrial or scientific laser, that attack scenario would have a *low* risk of technical failure because it was using a proven commercial technology. On the other hand, a terrorist attempting to build his own lightning machine would definitely fall into the *high* risk category because such a device would certainly qualify as an *elaborate, improvised weapon*.

Table 2
Risks Related to Technical Issues During an Attack

Risk of Failure	Attack Type
High	Attack uses elaborate, improvised weapons or other technologies (e.g., an improvised missile or a chemical or biological dispersal device).
Medium	Attack uses basic improvised weapons or other technologies (e.g., improvised explosive devices, a commercially manufactured poison that can be directly administered, or simple improvised communication modes).
Low	Attack uses proven commercial off-the-shelf weapons or other technologies (e.g., firearms, military weapons, commercial communication technology).

[18] The more moving parts the success of an operation depends on, the more likely a disconnect between one or more of those parts will cause it to fail. For example, a single attacker walking up to a person and shooting him or her has only one component. On the other hand, an attack in which terrorists use one bomb to blast their way through security to allow another bomber to enter a facility and blow it up from the inside has two, and breakdowns in timing between them or the failure of one would threaten the entire operation. The more closely different moving parts must happen in time, the greater the risk. An attack team required to successfully carry out two (or more) tasks at exactly the same time has a higher risk of failure (because of the coordination and skills required) than one that must conduct two tasks that need only occur within minutes or hours of each other.

The risk of technical failure applies to more pedestrian parts of operations as well, such as even getting to the target itself. An attacker using a car to drive to their target would have a *low* failure chance (automobiles are a proven commercial technology), but one that was flying there on a home-built powered parachute[19] would be in the *high* category.

With rating scales for all of the elements in Table 1 for ranking the ways emerging threat scenarios might break down at different phases of the operation, a security planner or analyst has the basis for comparing even very different types of operations.

Simple, single step attacks in which attackers take advantage of proven technologies would have mostly *low-risk* scores, highlighting the greater robustness of such operations where fewer things could go wrong. Even though it represents an exotic threat, some terrorist use of lasers (e.g., use of high-power industrial lasers in antipersonnel attacks or in attempts to incapacitate pilots in flight; see Bunker, 2008), would fall into this category because they require only the application of commercial off-the-shelf technologies in straightforward operational designs. Attacks with a low risk of failure merit more attention from security planners than scenarios with comparable consequences but higher chances of attacker failure.

More-complicated operations in which attackers have to rely more on improvised technologies or specialized skills or the success of which depends on factors beyond the terrorists' control (e.g., attack scenarios that rely on a crowd panicking to produce additional causalities) would receive more *medium risk* rankings.

Very complex terrorist scenarios (such as those one might see in movies or in television shows) that have many separate components, rely on high-technology weapons built by the terrorists themselves, are subject to many variables outside the attackers' control, and require split-second timing would pile up impressive totals of *high risk* scores, reflecting the difficulties an actual terrorist group would have pulling them off.[20] Compared with other scenarios with comparable consequences, scenarios that are very high risk for attackers would merit less attention from security planners because fewer adversaries would have the skills needed to pull them off and, if attempted, they have a greater chance of collapsing under the weight of their complexity and difficulty.

Just as was the case for identifying niche threats, determining that a particular scenario has a high chance of failure in many of its components does not mean that the operation will not happen. Scored in this manner, the September 11, 2001, terrorist plots would have fallen high on a number of risk scales, depending as they did on how the passengers on the flights reacted, on advanced piloting skills that the attackers had to acquire through training, and so on (see National Commission on Terrorist Attacks on the United States, undated). But success-

---

[19] SITE Intelligence Group translation of an al-Ekhlaas posting, "Remote-Controlled Cessna 128 SkyLane and Parachute Guides for Jihad," translation dated March 25, 2008.

[20] To illustrate this dynamic, we assessed the terrorist plot in the fourth season of the television series *24* based on episode descriptions from the Fox network's Web site (http://www.fox.com/24/episodes/season4/). Based on a conservative examination, that plot involved more than 50 separate steps, most of which had to occur within narrow time windows and included high-risk operations such as kidnappings of Cabinet-level officials, cyberattacks on large numbers of infrastructure targets, the complete destruction of a train with a vehicle bomb and the air-to-air engagement of a well-defended airliner (Air Force One) while recovering specific objects from the wreckage of both vehicles, the theft of defended military hardware (including a stealth fighter and a nuclear weapon), and integrating a stolen nuclear weapon into a customized missile for delivery to a distant target. Such a complex operation, the overall success of which hinged on the sequential completion of one nearly impossible task after another, may make for a gripping season of television but would be beyond the capabilities not just of any realistic terrorist group, but most nation-states as well.

fully carrying out operations with greater risk of failure requires more sophisticated attackers, meaning an operation with many *high-risk* rankings will be within reach for many fewer terrorist groups than simpler and more-robust attacks.

These comparisons of threats based on the details of the operations and the technologies involved are intentionally silent as to which particular terrorist group might try to carry them out, allowing threat scenarios to be compared without specifying from where a threat is coming—or might come—in some unknown future circumstance. Although of limited value for some evaluation purposes (e.g., the results of such a ranking should *not* be viewed as the probability a specific attack type will occur), this approach is useful because (1) emerging threat scenarios are often crafted without a specific attacker in mind during threat brainstorming and (2) intelligence that picks up chatter about possible future threats may or may not provide much insight into the actors considering them.

Though our discussion has focused on emerging threats—including scenarios as fanciful as terrorists constructing and deploying artificial lightning machines—our ranking approach can also be used to compare novel threats with operations that terrorists carry out routinely. For example, most simple "guns and bombs" terrorist operations would have *low-risk* scores, reflecting the robustness of most of the technologies involved and the simplicity of most of the operational designs. More-complex attacks, such as the use of advanced weapons such as the man-portable surface-to-air missiles mentioned in the introduction to this paper, would have somewhat higher risk scores given the greater sophistication of the technologies, the limits in the ability of groups to build expertise using them, and so on. Reflecting the fact that this analytical approach is designed to distinguish lower-risk emerging threats from ones that are more similar to these "tried and true" terrorist operations, there would be little overlap between the rankings of these operations and many of the attack modes terrorists have postulated in creative-writing exercises circulating on the Internet or the complex and intricate attacks more appropriate for a screenplay than the operational plans of any real-world terrorist group. As a result, security planners' attention and resources would be preserved for these more serious threats, and these others could be defensibly set aside.

Conclusions: Security Planning for the Niche and the Novel

Underlying this discussion of how to assess emerging threats is the belief that there is a value in stable security approaches that are acceptable to the people they are intended to protect and that are sustainable over time. If this is indeed the case, wrenching security efforts this way and that to respond to every potentially new threat that pops onto the national radar has a substantial cost. Although the new customized security measures implemented as part of a response to a novel threat have a direct cost, these measures also have indirect costs in terms of the disruption they may cause to ongoing security efforts and in terms of both public confidence and fear. The goal is therefore to strike the right balance between hypervigilance to every possible new threat and ignoring ways such threats might change over time.

But assuming that security planners are neither going to ignore emerging threats nor react to them all, reasonable ways to decide which ones to give attention to are needed. Based on our past work assessing a variety of different threats, we have suggested an approach that can act as a filtering mechanism for both the results of our own threat exploration and the constant

stream of possible future attacks our adversaries either publicize themselves or we discover through intelligence collection.

Identifying those novel threats that are best thought of as niches of larger threats makes it possible to filter out possible attacks that, while they might be new to terrorists, do not require new security plans or customized security measures. To the extent that such threats can be made lesser included cases of more general threats—and therefore be addressed by more-general security measures—the country benefits through more stable, simple security strategies at likely less cost. As was the case in our analysis of the threat of attacks using UAVs, it may be possible to prudently respond to a threat with just incremental changes to existing security activities. Resisting the temptation to put specific new security measures in place for each niche threat has an additional advantage when considering the fact that terrorist groups study and respond to the defenses deployed against them. The more specific the niche and the more specific the countermeasure aimed at addressing it, the easier it is for an attacker to respond by simply moving to a different niche of the same threat and rendering whatever investment was made in the countermeasure irrelevant (Jackson et al., 2007).

For new threats that are indeed new and cannot be as readily addressed by general security efforts, it also does not immediately follow that major changes in strategy or customized security measures are needed. Threats must be assessed systematically and prioritized because it is simply impossible to protect every possible target against every possible current and emerging threat. Attempting to protect against everything in a world of finite resources is remarkably similar to protecting against nothing, only much more expensive. Choices will always have to be made. We have described a process for using the details of threat scenarios—and how those details shape the likelihood of an attack failing—as method to compare very different hypothetical attacks. Such an approximate ranking method seeks to apply the concepts of risk analysis to situations where the data needed for accurate risk assessment simply does not exist. Though it is impossible to affirm that a particular type of attack will never happen, a scenario with a high failure chance would reasonably be of less concern than one with comparable consequences that was simple and straightforward.

Although a ranking scheme provides a way to prioritize threats, it does not provide absolute answers as to how far down that list of priorities security investments should be made as a hedge against possible future attacks. Such resource-allocation decisions involve additional considerations, and the choice could be very different at some targets than at others. As security planners shift from thinking through what emerging threats they should worry about to what to do in response, cost-effectiveness questions will also come into play: If it is possible to address some threats that are lower on the list at very little cost, it might be worth it to do so in spite of the relative likelihood of their taking place. But starting from a prioritized list will always be better than attempting to deal piecemeal with threats as different as terrorist insects, exploding remote-controlled planes, and artificial lightning and making decisions in isolation as to whether resources should be diverted from threats we can reasonably expect tomorrow to hedge against a very uncertain future.

References

Adams, Stephan, "Terrorists could use 'insect-based' biological weapon," *The Telegraph*, January 5, 2009. As of February 16, 2009:
http://www.telegraph.co.uk/earth/wildlife/4123782/Terrorists-could-use-insect-based-biological-weapon.html

Advanced Systems and Concepts Office (ASCO), Defense Threat Reduction Agency, "Research in Progress: Thwarting an Evil Genius," undated. As of February 16, 2009:
http://www.dtra.mil/asco/ascoweb/docs/Research%20Fact%20Sheet%20Thawting%20An%20Evil%20Genius.pdf

"Alberto Gonzales Holds a News Conference on the Miami Terrorist Cell Arrests," transcript of Justice Department news conference, CQ Transcripts, June 23, 2006.

"Al-Qaeda Online: Understanding Jihadist Internet Infrastructure," *Jane's Intelligence Review*, January 1, 2006.

Andrews, Arlan, "Science Fiction in the National Interest," transcript of interview with Brooke Gladstone, National Public Radio, *On the Media*, June 29, 2007. As of April 16, 2009:
http://www.onthemedia.org/transcripts/2007/06/29/07

Baird, R. A. "Pyro-Terrorism: The Threat of Arson-Induced Forest Fires as a Future Terrorist Weapon of Mass Destruction," *Studies in Conflict & Terrorism*, Vol. 29, No. 5, 2006, pp. 415–428.

Barrie, Allison, "Science Fiction Writers Help Government Prepare for Attacks of the Future," FOXNews.com, May 2, 2008. As of April 16, 2009:
http://www.foxnews.com/story/0,2933,353979,00.html

Bolkcom, Christopher, *Homeland Security: Defending U.S. Airspace*, Washington, D.C.: Congressional Research Service, CRS RS21394, June 6, 2006.

Bonomo, James, Giacomo Bergamo, David R. Frelinger, John Gordon, IV, and Brian A. Jackson, *Stealing the Sword: Limiting Terrorist Use of Advanced Conventional Weapons*, Santa Monica, Calif.: RAND Corporation, MG-510-DHS, 2007. As of April 16, 2009:
http://www.rand.org/pubs/monographs/MG510/

Bunker, R. J., "Terrorists and Laser Weapons: An Emergent Threat," *Studies in Conflict & Terrorism*, Vol. 31, No. 5, 2008, pp. 434–455.

Calvo, Dana, "Coming to an Army Near You," *Los Angeles Times*, July 19, 2002, p. A1. As of April 16, 2009:
http://articles.latimes.com/2002/jul/19/nation/na-institute19

Committee on Science and Technology for Countering Terrorism, National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, Washington, D.C.: National Academies Press, 2002.

Deshpande, N., "Pyro-Terrorism: Recent Cases and the Potential for Proliferation," *Studies in Conflict & Terrorism*, Vol. 32, No. 1, 2009, pp. 23–44.

Elias, Bart, "Lasers Aimed at Aircraft Cockpits: Background and Possible Options to Address the Threat to Aviation Safety and Security," Congressional Research Service, CRS RS22033, January 26, 2005.

Gormley, Dennis M., "UAVs and Cruise Missiles as Possible Terrorist Weapons," in James Clay Moltz, ed., *New Challenges in Missile Proliferation, Missile Defense, and Space Security*, Monterey, Calif.: Monterey

Institute of International Studies, Center for Nonproliferation Studies, Occasional Paper No. 12, July 2003, pp. 3–9.

———, "Unmanned Air Vehicles as Terror Weapons: Real or Imagined?" Issue Brief, Nuclear Threat Initiative, July 2005. As of April 16, 2009:
http://www.nti.org/e_research/e3_68a.html

Haimes, Yacov Y., *Risk Modeling, Assessment, and Management*, 2nd ed., Hoboken, N.J.: John Wiley and Sons, 2004.

Hall, Miami, "Sci-fi writers join war on terror," *USA Today*, May 31, 2007. As of April 16, 2009:
http://www.usatoday.com/tech/science/2007-05-29-deviant-thinkers-security_N.htm

Hsu, Spencer S. and Carrie Johnson, "Warning Boosts Security On N.Y. and D.C. Transit," *Washington Post*, November 27, 2008, p. A11.

Jackson, Brian A., Peter Chalk, Kim Cragin, Bruce Newsome, John V. 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, Calif.: RAND Corporation, MG-481-DHS, 2007. As of April 16, 2009:
http://www.rand.org/pubs/monographs/MG481/

Jackson, Brian A., David R. Frelinger, Michael J. Lostumbo, and Robert W. Button, *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*, Santa Monica, Calif.: RAND Corporation, MG-626-DTRA, 2008. As of April 16, 2009:
http://www.rand.org/pubs/monographs/MG626/

Jackson, Brian A., *Marrying Prevention and Resiliency: Balancing Approaches to an Uncertain Terrorist Threat*, Santa Monica, Calif.: RAND Corporation, OP-236-RC, 2008. As of April 16, 2009:
http://www.rand.org/pubs/occasional_papers/OP236/

Jane's Terrorism and Insurgency Centre, "Exploding Toy Planes—The Next Threat to Israeli Security?" Coulsdon, Surrey, United Kingdom, February 24, 2003.

"Jihadists Offer Hypothetical Scenarios, Targets for Attack," al-Fallujah posting, SITE Intelligence Group translation, dated February 16, 2009.

Karmon, Ely, "Hizballah as Strategic Threat to Israel," *Heartland—Eurasian Review of Geopolitics*, Vol. 2-2005, July 2005, pp. 22–48.

Lal, Rollie and Brian A. Jackson, "Change and Continuity in Terrorism Revisited: Terrorist Tactics, 1980–2005," *The MIPT Terrorism Annual 2006*, Oklahoma City, Okla.: MIPT, 2006. As of April 16, 2009:
http://www.terrorisminfo.mipt.org/pdf/2006-MIPT-Terrorism-Annual.pdf

Lockwood, Jeffery, *Six-Legged Soldiers: Using Insects as Weapons of War*, New York: Oxford University Press, 2008.

Magnuson, Stew, "Science Fiction Mavens Offer Far Out Homeland Security Advice," *National Defense*, March 2008. As of April 16, 2009:
http://www.nationaldefensemagazine.org/archive/2008/March/Pages/ScienceFictionMavensOfferFarOutHomelandSecurityAdvice.aspx

McGill, William, "Six Papers on Six Different 'Emerging' Terrorist Threats" blog entry, *McGill Research Blog: Thoughts on Risk, Uncertainty and Everything Else,* May 28, 2008. As of April 16, 2009:
http://www.professormcgill.com/blog/2008/05/

Miasnikov, Eugene, "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects," Moscow, Russia: Center for Arms Control, Energy, and Environmental Studies, Moscow Institute of Physics and Technology, 2005.

Mintz, John, "Homeland Security Employs Imagination: Outsiders Help Devise Possible Terrorism Plots," *Washington Post*, June 10, 2004, p. A27.

National Commission on Terrorist Attacks on the United States, "Outline of the 9/11 Plot," Staff Statement No. 16, undated. As of April 16, 2009:
http://govinfo.library.unt.edu/911/staff_statements/staff_statement_16.pdf

———, *The 9/11 Commission Report*, 2004.

Schneier, Bruce, "Announcing: Movie-Plot Threat Contest," blog entry, *Schneier on Security,* April 1, 2006. As of April 16, 2009:
http://www.schneier.com/blog/archives/2006/04/announcing_movi.html

———, "Announcing: Second Annual Movie-Plot Threat Contest," April 1, 2007. As of April 16, 2009:
http://www.schneier.com/blog/archives/2007/04/announcing_seco.html

———, "Portrait of the Modern Terrorist as an Idiot," in *Schneier on Security*, Indianapolis, Ind.: Wiley Publishing, Inc., 2008.

Shooman, M. L., "Terrorist Risk Evaluation Using *A Posteriori* Fault Trees," in *Reliability and Maintainability Symposium, 2006*, 2006, pp. 450–455.

Transportation Security Administration, "Remote Control Vehicles and Other Toys," Web page, September 28, 2007. As of April 16, 2009:
http://www.tsa.gov/press/happenings/remote_control_vehicles.shtm

"Troops Seize Rebels' Explosive Planes," Houston Chronicle News Services, August 27, 2002.

U.S. Army, *Risk Management*, Field Manual 100-14, April 23, 1998.

Verton, Dan, "A View to a Kill: Terrorists and UAVs," *Homeland Defense Journal*, May 2005, pp. 10–14.