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

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

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.