This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Breaching the Fortress Wall

Understanding Terrorist Efforts to Overcome Defensive Technologies

Brian A. Jackson • Peter Chalk • R. Kim Cragin
Bruce Newsome • John V. Parachini • William Rosenau
Erin M. Simpson • Melanie Sisson • Donald Temple

Prepared for the Department of Homeland Security

Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

This research was sponsored by the United States Department of Homeland Security and was conducted under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment.

Library of Congress Cataloging-in-Publication Data

Breaching the fortress wall : understanding terrorist efforts to overcome defensive technologies / Brian A. Jackson ... [et al.].
p. cm.
"MG-481."
Includes bibliographical references.
ISBN 0-8330-3914-8 (pbk. : alk. paper)
1. War on Terrorism, 2001–—Technology. 2. Security systems. 3. Terrorism—Prevention. 4. Terrorism—Prevention—Case studies. 5. Terrorism—Case studies. 6. National security. I. Jackson, Brian A. (Brian Anthony)

HV6431.B737 2007
363.325'72—dc22

2006001721

Cover design by Eileen Delson La Russo
Photo by TSgt Cedric H. Rudisill, U.S. Air Force

Published 2007 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

The level of threat posed by a terrorist group[1] is determined in large part by its ability to build its organizational capabilities and bring those capabilities to bear in violent action. As part of homeland security efforts, technology systems play a key role within a larger, integrated strategy to target groups' efforts to do so and protect the public from the threat of terrorist violence. Although many types of technology have roles to play in the overall effort to fight terrorism, this analysis focuses on a class of tools that we call *defensive technologies*—the systems and approaches deployed to protect an area and its citizens from terrorism by discovering and frustrating the plans of terrorists operating therein. The technologies that we have defined as defensive technologies can be organized into five primary classes based on their intended impact on the terrorist adversary:

- **Information acquisition and management.** These tools include surveillance technologies and practices that enable law enforce-

[1] Although some of the substate groups discussed in this book use tactics that are not purely terroristic in nature—for example, mixing traditional military operations against opposing security forces with terrorist bombings or assassinations—we use the terms *terrorism* and *terrorist violence* as generic descriptors of the violent activities of substate groups.

In this book, we adopt the convention that *terrorism* is a tactic—the systematic and premeditated use, or threatened use, of violence by nonstate groups to further political or social objectives to coerce an audience larger than those directly affected. With terrorism defined as a tactic, it follows that individual organizations are not inherently *terrorist*. We use the terms *terrorist group* and *terrorist organization* as shorthand for "group that has chosen to use terrorism."

ment and security organizations to gather information on terrorist individuals, vehicles, and behaviors; to monitor sites and areas (including border information systems aimed at excluding terrorists from the country); to detect concealed weapons and operations in progress; and to maintain the profiles, databases, and systems needed to manage and use such information once collected.

- **Preventive action.** Technologies in this category include systems to counter specific terrorist weapon systems (e.g., radio-detonator jamming, antimissile systems) and systems designed to prevent terrorist access to money, weapons, technologies, and other resources or knowledge.
- **Denial.** Such approaches include traditional hardening of potential targets (e.g., setbacks, blast walls, reinforced windows, or other structures); design changes in potential targets to make them less susceptible to attack (e.g., increasing the robustness of infrastructure systems, immune buildings); hardening of the population (e.g., psychological preparedness efforts, vaccination); and security or guard force deployment.
- **Response.** These technologies are designed to provide multiple capabilities, including defeating operations in progress (e.g., explosive ordnance disposal teams); ensuring that emergency responses are adequate to treat casualties and limit the spread of damage from attacks in progress; coordinating response operations for increased effectiveness; making antidotes or other treatment methods for specific types of terrorist attacks readily available; and providing risk communication capabilities, which can be used to shape public responses to minimize the effects of an attack.
- **Investigation.** Technologies in this domain include forensic science and other investigative and identification technologies to analyze terrorist weapons, track and apprehend suspects, support prosecution of individuals responsible for terrorist operations, or enable other sovereign action against individuals or terrorist organizations.

These do not represent the only technologies relevant to efforts to combat terrorism. A range of technologies applied in more proactive or offensive operations against terrorist groups—including military weaponry and similar technologies—are not included within the scope of this book. It should also be noted that the distinction between offensive and defensive technologies is admittedly ambiguous; the same intelligence-gathering system deployed in a defensive mode to detect terrorist operations in progress could clearly gather information supporting offensive operations against terrorist organizations.

Although the contributions that technology can make in combating terrorism can be considerable, it should be noted that technology is only one of many tools for combating terrorism. For example, virtually all sources consulted for this book emphasized the preeminence of direct human intelligence—through infiltration of terrorist organizations or the recruitment of their members as agents—as the most important element of an effort to combat terrorists' activities.[2] The emphasis of this book on technical systems should not be interpreted as contradicting this view—rather, the work described here should be seen as part of a multifaceted effort against terrorism to ensure that technology complements other efforts as effectively and efficiently as possible.

Terrorist Efforts to Overcome Defensive Measures

Although the variety of defensive technologies available enables broad-based targeting of terrorists' activities, defending a nation against terrorism is not a one-sided game. Given the potential for defensive technologies to constrain the capabilities of terrorist groups and limit their operational freedom, these organizations are acutely aware of government efforts to deploy them and actively seek ways to evade or counteract them. This measure-countermeasure, move-countermove dynamic is inherent in contests between organizations and, to the extent that

[2] Personal interviews with former law enforcement officials, England (May 2005) and with local officials, Indonesia, the Philippines, Singapore, and Thailand (March–April 2005).

the terrorists' efforts are successful, can significantly reduce or eliminate the value of defensive technologies.[3]

This book focuses on understanding terrorists' countertechnology efforts by drawing on relevant data from the history of a variety of terrorist conflicts and applying that information to the broader technological questions relevant to current homeland security efforts. These cases were selected for examination:

- **Palestinian terrorist groups.** In Israel, a variety of Palestinian terrorist groups (including Hamas, Palestinian Islamic Jihad [PIJ], and the al-Aqsa Martyrs Brigade) face a strong challenge from Israeli defensive measures, including surveillance assets and the barrier wall being constructed to prevent entry into Israel from the West Bank and Gaza. These groups have adopted a number of responses, including avoidance and camouflage, a variety of approaches to avoid the defensive wall, and new weapons that maintain their offensive capabilities.
- **Jemaah Islamiyah (JI) and affiliated groups.** In Southeast Asia, JI and its affiliated groups face varied defensive measures across the multiple countries in which they operate. These groups have adopted deception and forgery to maintain their ability to move from country to country and operational and technical ways to evade weapon detection technologies, and they have made other changes in target selection and operations to preserve their capabilities and operational freedom.
- **Liberation Tigers of Tamil Eelam (LTTE).** In Sri Lanka, LTTE used suicide terrorism for high-priority offensive missions. A number of defensive measures were put in place, including operative profiling, detection methods, and hardening potential targets of attack. LTTE responded by modifying its operational practices to include out-of-profile operatives, evading detection tech-

[3] Although examining this was beyond the scope of this study, it should also be noted that the nature of the defensive technologies available and their application also shapes the "defender's perspective" about appropriate responses to the terrorist threat and assumptions about terrorist behavior.

niques or hiding the signatures they were designed to detect, and improving its techniques for penetrating defenses.
- **Provisional Irish Republican Army (PIRA).** In the United Kingdom, PIRA faced a diversity of defensive technologies aimed at undermining all facets of its operations. Through innovation and various operational approaches, PIRA developed strategies to counter security force information gathering and measures to jam or neutralize the group's weapons, protections around key targets, and even the ability of police to investigate and gather evidence after attacks.

Although the terrorist groups developed a wide variety of countertechnology measures for specific defensive technologies, many specific countermeasures they adopted have common elements that permit us to define a smaller number of fundamental countertechnology strategies. The groups applied these strategies, singly or in combination, when faced with a defensive technology threat. They are as follows:

- **Altering operational practices.** By changing the ways in which it carries out its activities or designs its operations, a terrorist group may blunt or eliminate the value of a defensive technology. Such changes frequently include efforts to hide from or otherwise undermine the technology's effect.
- **Making technological changes or substitutions.** By modifying its own technologies (e.g., weapons, communications, surveillance), acquiring new ones, or substituting new technologies for those currently in use, a terrorist group may gain the capacity to limit the impact of a technology on its activities.
- **Avoiding the defensive technology.** Rather than modifying how it acts to blunt the value of a defensive technology, a terrorist group may simply move its operations to an entirely different area to avoid it. Such displacement changes the distribution of terrorism, and, although this may constitute successful protection in the area in which the defensive technology is deployed, the ability to shift operations elsewhere limits the influence that the technology can have on the overall terrorist threat level.

- **Attacking the defensive technology.** If appropriate avenues are available, a terrorist group may seek to destroy or damage a defensive technology to remove it as a threat.

Although specific terrorist countertechnology efforts occasionally may fall into more than one of these classes, this taxonomy of strategies provides a systematic way to consider how terrorist organizations might respond to a newly deployed defensive measure.

Addressing Terrorist Countertechnology Efforts in Homeland Security Planning and Decisionmaking

The potential for terrorist groups to develop and deploy countermeasures for new defensive technologies must be addressed to ensure that protective efforts are effective and resources are allocated wisely.

Lessons for the Design of Defensive Technologies

To ensure that new defensive technology systems provide the greatest potential security benefits, they must be designed with terrorist countertechnology behaviors and past successes in mind. The efforts of the groups studied here suggest four techniques or approaches to use in developing plans for new defensive technologies.

- **Red teaming technology systems.** Given terrorist countertechnology behaviors, there is a clear need to test or "red team" new technologies, drawing on the terrorists' available palette of counterstrategies, to assess the limits of a technology before it is built and deployed.
- **Assessing adversary information requirements.** There is a clear need to analyze the information an adversary would need to circumvent the defensive technology and assess how the adversary might gain access to that information.
- **Designing flexibility into defensive technologies.** For most defensive measures, terrorist groups will eventually develop counterstrategies that limit their value. As a result, systems that are

flexible—that are not locked into specific modes of operation and can adapt themselves—may provide an added value.

- **Anticipating how technologies will guide terrorist adaptation.** When challenged by a new defensive technology, a successful terrorist effort to adapt may actually build it into a more potent threat than existed before the technology was deployed. To limit the potential for such unintended consequences, the design process for defensive systems should explore the effect of terrorist countertechnology responses not only on the value of the defensive systems, but also on the group overall and the nature of the threat it poses.

Lessons for Planning the Technological Components of Homeland Security Efforts

When terrorists are successful in countering all or part of the functioning of a defensive technology, the utility of the system may be significantly reduced or lost entirely. Such losses devalue the costs[4] society pays to design, produce, field, use, and maintain the technology.[5] As a result, potential countertechnology efforts need to be included in planning in three critical areas:

- **Include terrorist countertechnology efforts in programmatic and cost-benefit analyses of defensive systems.** In assessing a novel technology and its cost, the risk that its development and deployment might fail to deliver promised benefits is an established component of management planning. Like the competitive risk that another firm will develop a superior product, rendering a company's investments meaningless when both reach the

[4] The concept of costs includes not only financial and materiel costs but also auxiliary costs such as any reductions in privacy and civil liberties or costs paid in time or inconvenience by the public as a result of implementation of the security measures.

[5] For a nation as large and populous as the United States, these costs can be considerable. For example, at the time of this writing, major initiatives regarding border security and critical infrastructure protection are under consideration. Given the scope of both problems and the resources needed to implement solutions, considering how terrorists might act to counter protective measures that are put in place is clearly critical.

market, successful terrorist countertechnology efforts can similarly destroy the competitive advantage of a new defensive system. This *countertechnology risk* must be assessed and included as part of program management above and beyond the technological and other risks inherent in the effort itself.

- **Consider the relative costs of countering a technology and the cost of the technology itself.** The cost that a defensive technology can impose on a terrorist group—in effort and resources required to either withstand or counter its effects—is one measure of its value. If the cost is great enough, the technology's effect can be decisive. The cost that the nation should be willing to pay for a technology system must be related to its potential effect on its adversaries. When a technology can be countered with little investment on the part of the terrorist, the balance is in the terrorists' favor. This is particularly problematic when a group can access countertechnology strategies from other sources—for example, through technology transfer from other terrorist groups—that could significantly reduce or eliminate costs to the group.[6]
- **Address multistep countertechnology activities in assembling security technology portfolios.** Although this discussion focuses predominantly on single-step interactions between terrorist groups and defensive technologies—a single response by a group to a deployed technology—real conflicts are multistep contests. In consecutive iterations of measure and countermeasure competition, the potential exists for the terrorist to eventually overwhelm even the most adaptable defensive technology and reduce it to uselessness. If and when that occurs, new options will be needed. Given the potential for such "adaptive destruction" of individual security approaches, planning must consider defensive technologies as a portfolio, maintaining possibilities for alternative approaches in the event that currently effective technologies are neutralized.

---

[6] A companion publication produced during this research project, *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies*, by Kim Cragin, Peter Chalk, Sara A. Daly, and Brian A. Jackson, addresses this topic in detail.

Conclusions

Although technologies can provide an edge in the effort to combat terrorism, that edge can be dulled by terrorist countertechnology efforts. An understanding of past terrorist efforts to counter defensive technologies underscores the complexity of designing new systems to protect society from the threat of these violent organizations. This analysis suggests that, in designing protective measures, it should not immediately be assumed that the newest and most advanced technologies—the highest wall, the most sensitive surveillance—will best protect society from terrorist attack. Drawing on common metaphors for defensive efforts, a fortress—relying on formidable but static defensive measures—is a limiting strategy. Once a wall is breached, the nation is open to attack. Depending on the adaptive capabilities of the adversary, a defensive model built of a variety of security measures that can be adjusted and redeployed as their vulnerable points are discovered provides a superior approach to addressing this portion of terrorist behavior. However, whatever combination of models and measures is chosen, it is only through fully exploring an adversary's countertechnology behaviors that vulnerabilities in a nation's defenses can be discovered and the best choices made to protect the nation from the threat of terrorism.