Research Brief

RAND Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

Getting Inside the Terrorist Mind

RAND RESEARCH AREAS
THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE
WORKFORCE AND WORKPLACE

Abstract

Being able to understand the motivation of al Qaeda and other groups can help nations better disrupt, defend against, and prepare for and anticipate terrorist attacks. Three new studies, relying on a case study approach, offer insights into the terrorist mindset, focusing, in particular, on how terrorists try to get around defensive technologies, share technologies among themselves, and prioritize their targets.

In fighting any war, it helps to "get inside the enemy's mind." In the past, that meant understanding the motivations of a monolithic state enemy like the Soviet Union. But doing that today in combating terrorism is far more challenging, because, in battling al Qaeda and other groups, the United States is dealing with amorphous, ever-changing terrorist organizations.

Putting ourselves in the terrorists' shoes could help us answer a number of questions: When we put in place technological defenses against terrorists, what do they do to get around them? When terrorists seek to develop new technologies, how do they work with other terrorist groups to share information and technologies? And when terrorists target the United States, what guides their preferences?

Three new RAND Corporation studies seek to help answer these three questions, relying on a case study approach of al Qaeda and other terrorist groups to draw out some applicable lessons for policy planning.

Measure-Countermeasure: Defending Against Terrorist Attacks

Nations employ five basic types of defensive technologies to protect their citizens from terrorism by discovering and frustrating the plans of terrorists: information acquisition and management, preventive action, denial, response, and investigation.

But as nations use defensive measures, terrorists use countermeasures in response. Relying on case studies of four terrorist groups, researchers showed that terrorists (1) change how they carry out activities or design operations; (2) modify their own technologies, acquire new ones, or substitute different technologies for the ones they currently use; (3) avoid the defensive technology; or (4) destroy or damage the defensive technology.

Given that terrorists have been successful in using such countermeasures, the analysis suggests that, in designing protective measures, the United States should not immediately assume that the newest and most advanced technologies—the highest wall, the most sensitive surveillance—will best protect nations from terrorist attacks. Relying on a "fortress"—formidable but static defensive measures—is a limiting strategy. Assuming instead that adversaries are adaptive, it makes more sense to rely on a defensive model—a variety of security measures that can be adjusted and redeployed as terrorists discover their vulnerable points.

Disrupting Terrorist Technology- and Knowledge-Sharing

The attacks on al Qaeda after September 11, 2001, have changed the nature of the terrorist threat the United States is facing, leading some terrorist groups that lack the global reach of a pre-9/11 al Qaeda to form regional alliances and to share knowledge and technologies. Relying on case studies of 11 terrorist groups in three regions, researchers sought to understand what made for successful knowledge and technology exchanges as a way of determining vulnerabilities in these technology exchanges. Analysis pointed to three key conclusions.

Threat Assessments Must Focus on Intergroup Dynamics. This includes technology exchange. Terrorist groups thought potential

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of published, peer-reviewed documents.

Corporate Headquarters
1776 Main Street
P.O. Box 2138
Santa Monica, California
90407-2138
TEL 310.393.0411
FAX 310.393.4818

© RAND 2007

www.rand.org

gains or costs in operational capabilities more important than ideological similarities when deciding whether to participate in technological exchanges; thus, threat assessments should focus on operational as well as strategic motivations for alliances. Threat assessments should monitor individuals not just with chemical, biological, radiological, or nuclear expertise, but also those with expertise in conventional attack modes, such as remote-detonation technologies, rockets and missiles, improvised explosive devices, and converted field ordnance.

Terrorists' Innovation Processes Should Be Disrupted. This will reduce the potential for a successful technology exchange. For example, governments have provided safe havens as incentives to get terrorists to participate in peace negotiations, but such safe havens facilitate technology transfers. Tightening porous borders can also help disrupt technology exchanges.

Policies Should Disrupt Trust Among Terrorist Groups. Policies such as blocking payment transfers can affect a terrorist group's cost-benefit analysis of getting involved in technology exchanges.

Prioritizing Targets of Terrorist Attacks

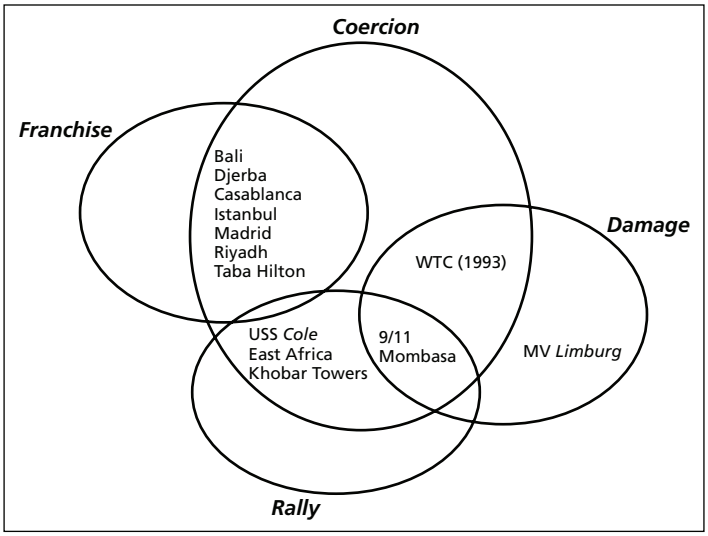
Al Qaeda seeks a restored Caliphate free of Western influence. Clearly, it uses terror as its means. But how does terrorism serve al Qaeda's ends? Understanding *how* al Qaeda's leadership thinks terrorism gets it closer to the Caliphate might suggest what U.S. targets it may seek to strike and why.

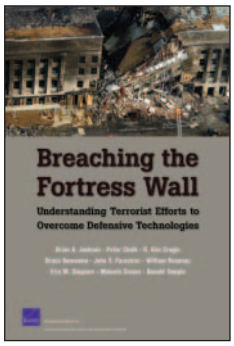
This research posits four hypotheses to link means and ends. The *coercion* hypothesis suggests that terrorists seek to cause pain, notably casualties, to frighten the United States into pursuing favorable policies (e.g., withdrawing from the Islamic world). The *damage* hypothesis argues that terrorists want to damage the U.S. economy to weaken its ability to intervene in the Islamic world. The *rally* hypothesis holds that terrorism in the United States is meant to attract the attention of potential recruits and supporters. Conversely, the *franchise* hypothesis argues that today's jihadist terrorists pursue their own, often local, agendas, with, at most, support and encouragement from al Qaeda itself. RAND researchers examined each hypothesis by analyzing 14 major terrorist attacks (shown in the figure) and al Qaeda's own statements, as well as by surveying terrorism experts.

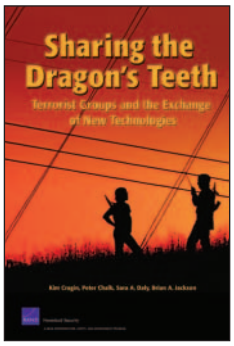
Such research suggests that the *coercion* and *damage* hypotheses are most consistent with prior attack patterns, expert opinion, and al Qaeda's statements. Although the *franchise* hypothesis fits most of the post-9/11 attacks, unless franchises are active in the United States, that fact may not indicate what the next attack in the United States might look like.

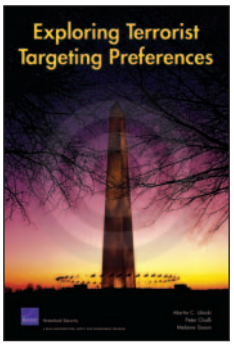
Indeed, given al Qaeda's current resource limitations, such an attack may well favor using suicide bombers and could focus on soft (poorly defended) targets. Attacks on the food industry, particularly the agricultural sector, and the use of radiological dispersion devices merit attention. ■

Attack Distribution by Hypothesis









This research brief describes work done for the Homeland Security Program within RAND Infrastructure, Safety, and Environment and documented in three books: *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, by Brian A. Jackson, Peter Chalk, R. Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie Sisson, and Donald Temple, MG-481-DHS (available at http://www.rand.org/pubs/monographs/MG481/), 2007, 182 pp., $25, ISBN: 978-0-8330-3914-9; *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies*, by R. Kim Cragin, Peter Chalk, Sara A. Daly, and Brian A. Jackson, MG-485-DHS (available at http://www.rand.org/pubs/monographs/MG485/), 2007, 136 pp., $20, ISBN: 978-0-8330-3915-6; and *Exploring Terrorist Targeting Preferences*, by Martin C. Libicki, Peter Chalk, and Melanie Sisson, MG-483-DHS (available at http://www.rand.org/pubs/monographs/MG483/), 2007, 130 pp., $20, ISBN: 978-0-8330-3913-2. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

RAND Offices
Santa Monica, CA • Washington, DC • Pittsburgh, PA • Jackson, MS • Cambridge, UK • Doha, QA

RB-9258-DHS (2007)

Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of individual published, peer-reviewed documents or of a body of published work.

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore RAND Homeland Security

View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use.