



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.

[Jump down to document](#) ▼

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

[Purchase this document](#)

[Browse Books & Publications](#)

[Make a charitable contribution](#)

For More Information

Visit RAND at www.rand.org

Explore [RAND Homeland Security Program](#)

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. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see [RAND Permissions](#).

This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL REPORT

Network Technologies for Networked Terrorists

Assessing the Value of Information
and Communication Technologies
to Modern Terrorist Organizations

Bruce W. Don, David R. Frelinger, Scott Gerwehr,
Eric Landree, Brian A. Jackson

Prepared for the Department of Homeland Security



Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

The research described in this report was prepared for the United States Department of Homeland Security and conducted under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment.

Library of Congress Cataloging-in-Publication Data

Network technologies for networked terrorists : assessing the value of information and communications technologies to modern terrorist organizations / Bruce W. Don ... [et al.].

p. cm.

Includes bibliographical references.

ISBN 978-0-8330-4141-8 (pbk.)

1. Terrorism—Technological innovations. I. Don, Bruce W.

HV6431.N4818 2007

363.3250285—dc22

2007003787

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.

© Copyright 2007 RAND Corporation

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from RAND.

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

Understanding how terrorists conduct successful operations is critical to countering them. It has become apparent that terrorist organizations are using a wide range of technologies as they plan and stage attacks. Most examinations of the technology used to enable terrorist operations focus on their weapons—the instruments directly responsible for death and destruction in their attacks—and how new technologies might increase the resulting damages, injuries, and fatalities. However, successful terrorist operations involve more than simply employing weapons to produce their physical effects. Information gathering, assessment and planning, coordination, logistics, and command capabilities all play a role in delivering the terrorist's weapon to its intended target with deadly effect, and the very existence of a terrorist organization is based on recruiting and information campaigns. As a result, understanding the role that such technologies play and the net effect of their use requires an understanding not only of the technology, but also of the purpose and manner in which the technology is used and of the operational actions and responses of the security forces and the terrorists. To gain such an understanding, the study has taken a broad scope in assessing the issue.

Study Scope and Purpose

This analysis focuses on the potential application of information and communication technologies that may be used across the full range of activities that make up terrorist operations and whether these applications can lead to new and different approaches to terrorist operations. Its purpose is to identify which of these network technologies terrorist organizations are likely to use in conducting their operations and to suggest what security forces might do to counter, mitigate, or exploit terrorists' use of such technologies.

To highlight the merger of software and computer technologies with communication and display technologies that digitalization has made possible and to encourage thinking beyond military technologies, this report uses the term *network technologies* to describe what are referred to as command, control, communication, computer, intelligence, surveillance, and reconnaissance (C4ISR) technologies in military parlance, as well as the consumer-oriented technologies that can often provide the functionality needed for terrorist operations. These network technologies can include connectivity technologies (e.g., wireless routers), mobile computing (e.g.,

laptop computers), personal electronic devices (e.g., personal digital assistants and cell phones), IT services and Internet access, and video recording, among others.

Approach to the Analysis

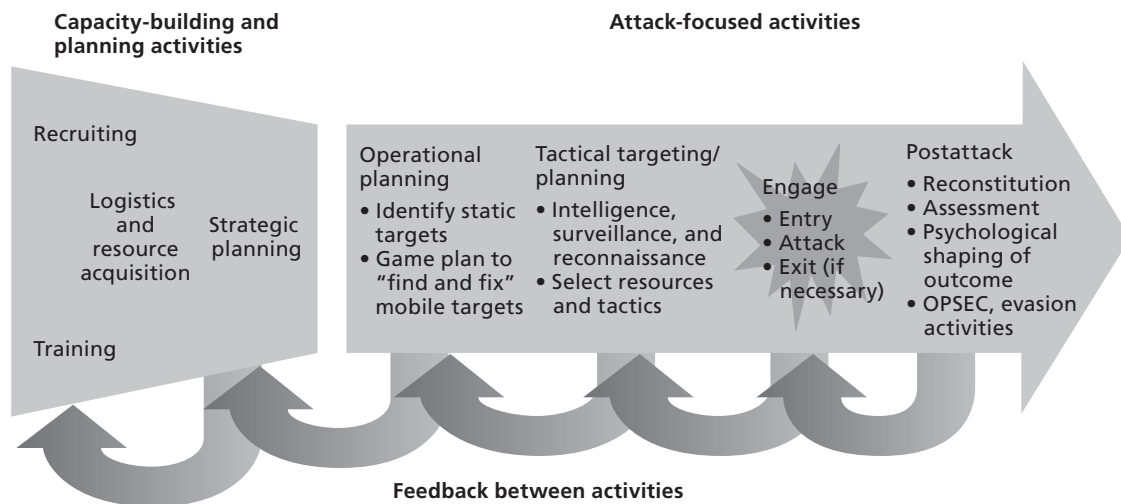
The RAND research team used five research questions to guide the analysis of the terrorist use of network technologies and to identify effective ways for security forces to counter their use.

1. What could terrorists do with network technologies?
2. Which network technologies are most attractive to terrorists?
3. How would specific network technologies fit within terrorist groups' broader approaches to acquiring and using technologies?
4. What should security forces do to counter this?
5. What conclusions and recommendations can be drawn from this analysis?

First, the team developed a terrorist activity chain shown in Figure S.1. It is a logic model that describes the activities that make up most terrorist operations and explains how these activities relate to one another.

Next, the team examined terrorist use of network technologies for the elements of the terrorist activity chain to discover which of the activities could benefit from terrorist use of network technologies and which network technologies might promise the most substantial benefits. To do this, the study team based its investigation on the following questions:

Figure S.1
The Terrorist Activity Chain



NOTE: OPSEC = operational security.

RAND TR454-S.1

- How have terrorists used network technologies to support terrorist operations *in the past*?
- How are terrorists now using network technology to support their *current operations*?
- What uses of network technologies may terrorists be *expected to make in the future*, and might such use lead to revolutionary changes in future operations?

The next step was to identify which network technologies were most attractive to terrorists. The team analyzed the types of network technologies that would be most useful for a given terrorist activity, whether they would be practical to acquire, and whether any technologies might offer revolutionary changes. We base our assessment on the expectation that terrorists will adopt a technology if it can confer one of two types of benefits with reasonable risks:

1. those that improve the organization's ability to carry out activities relevant to its strategic objectives, such as recruiting and training, or
2. those that improve the outcome of their attack operations.

The team then developed a structured way of thinking about how terrorists acquire technologies and the role that specific network technologies play within groups' technology strategies. These technology strategies are as follows:

1. *Invest in specialized technology, in pursuit of a significant effect on attack outcomes or perhaps operational efficiency.* Typically, such technologies require some parts of the organization to specialize for effective acquisition and employment.
2. *Either rely on versatile technologies that can be used many ways or pursue a wide variety of individual technologies, with the expectation of a moderate effect on operational efficiency and, perhaps, some positive benefits for attack outcomes.* Groups frequently acquire technologies relevant to both these strategies externally from legal or illegal market sources.
3. *Use technology opportunistically, with the expectation that technology will only contribute to attack outcomes and operational efficiency in minor ways.* Such a strategy may also result in little organizationwide vulnerability to technology failures, countermeasures, or exploitation.

These strategies summarize the approaches that have been successful for terrorist organizations in light of the basic characteristics of *both* the technology and the manner in which it could be used. They crudely incorporate a broad set of factors that are fundamentally related to one another: the nature of the technology, the operational environment in which it would be useful, the general effect of its use, and the acquisition approach it requires. As a result, they provide a simple model that can serve as a framework for evaluating the effectiveness of alternative ways for security forces to respond to these general approaches to technology by a terrorist organization.

Finally, the team evaluated how to best counter terrorists' use of network technologies. This required the research team to assess and compare the benefits and risks of different countermeasure options. To do this, we developed a framework that considers three basic factors:

1. the role that a specific network technology plays within a terrorist group's overall technology strategy
2. the balance of benefits and risks of technology use from both the terrorists' and security forces' perspective
3. options for security forces to counter terrorists' use of network technologies.

This framework allowed the team to compare the payoff for each combination of network technology used by terrorists and countermeasure available to security forces.

As any analysis, this approach has its limitations. Because terrorists will not necessarily use technology or conduct operations in the ways that they have in the past, the conclusions of this analysis are limited most importantly by how insightful the research team has been in two areas: envisioning how clever terrorists can be in their future use of network technology and understanding the limitations that realistically constrain future terrorist operations. Unforeseen new uses are certainly possible, given the rapid pace of technology development, and future operations involving terrorists may be very different from current operations. However, the team believes that the approach we have used for this analysis is uncomplicated and flexible enough to be used on a continuing basis to examine startlingly new or evolving situations. This need for update and review is the basis for our recommendation suggesting that DHS put in place a system to do this on an ongoing basis.

Conclusions

Future network technologies are most likely to result in real but modest improvements in overall terrorist group efficiency but not dramatic improvements in their operational outcomes. This results largely from the circumstances under which terrorist groups must operate, particularly in the homeland security arena, and the carefully planned and scripted style of their attacks. These groups must operate through inherently fragile, clandestine terrorist cells that have resource limitations, a need for secrecy for survival, and a need for surprise and scripted attacks for operational effectiveness. All of these considerations result in an operational style that favors uncomplicated operations with concrete effects and minimal core needs for the capabilities that network technologies provide.

Terrorists will most likely acquire network technologies for the versatility and variety that they offer and will use them to enhance the efficiency and effectiveness of their supporting activities. The effect of these kinds of technologies will be to make their activities more efficient or effective. That is, they will be able to carry them out with fewer people or better results. Thus, they might be able to get by with fewer people devoted to recruiting new members because one person might be able to recruit more new members.

Attempting to preclude terrorists from getting the types of technology they want will not be practical, and developing direct counters to them will unlikely yield a high payoff. Network technologies that feature versatility and variety are largely driven by the worldwide consumer and commercial markets. It is not practical to keep these kinds of technologies out of the hands of terrorists. Such technologies can simply be bought off the shelf. Even if it were possible to deny terrorists these technologies, the benefits of doing so would probably not justify the costs of the effort required to block their acquisition.

Exploitation seems the more promising option. The best use of resources for those attempting to counter terrorist operations would seem to be developing ways to exploit the network technologies that terrorists will continue to use. As is the case with most people who use cell phones and computers, most terrorists do not have detailed knowledge of how those devices work. Therefore, it may be possible for sophisticated security forces to alter them in ways that enable security services to identify the users or their locations or to monitor their transmissions. This approach also targets a key vulnerability: an absolute need of terrorist organizations to remain hidden.

Even though there do not appear to be any network technologies that offer revolutionary capabilities in the immediate future, security services need to monitor the development of technologies in the event that such a capability emerges. One area that might require careful monitoring would be network technologies that enable terrorist organizations to assume the identity of government personnel (perhaps electronically) or take over media outlets. Even though it is unlikely that they could do this for a sustained period, even a short takeover could be terribly disruptive, particularly in densely populated urban areas.

Recommendations

In light of the above conclusions, the research team recommends the following actions.

Design a system to address terrorist use of network technologies. Security organizations need a process that determines whether new network technology has been or is likely to be introduced into terrorist operations, identify its effect, select a response, gather needed resources, and implement an appropriate counter to the technology's use, and to do all of these in a timely manner.

Acquire and sustain people with the core competencies needed to make the system work. Homeland security forces and other organizations involved in combating terrorism need the following core competencies to address the use of network technologies by terrorist organizations:

- an understanding of the technologies themselves, particularly the technical challenges of exploitation and the operational limitations imposed by terrorist and security force operations
- an ability to track terrorist adoption, use, or avoidance of particular technologies
- a capability to determine which responses, or which mix of responses, is most appropriate in light of security force goals, and

- the capacity to develop plans and execute operations to actuate the selected responses as part of the larger strategy to counter terrorist organizations.

Take the initial steps needed to implement such a system promptly. Initial actions that can quickly provide a good basis for a system that can counter terrorist organizations' network technology use include the following DHS activities:

- Continue and accelerate the recruitment, retention, and professional education of technically skilled personnel who understand network technologies.
- Define the requirements for intelligence collection that focuses on terrorist use of network technologies and communicate them to the intelligence community.
- Create an effort within the homeland security research program to examine terrorist use of network technologies.
- Develop the capability to determine whether to exploit the use of the network technology; develop and employ operational countermeasures to the network technology; disrupt the process by which terrorist groups acquire new network technologies; or determine that other counterterrorism efforts are more effective than a response.
- Develop a capability to respond quickly with technical and engineering solutions to counter or exploit emerging network technology being used by terrorists.

These actions should provide a basic capability within DHS that can contribute to the homeland security mission in the short term and that can be shaped to provide the most efficient and effective ways to address this threat over the longer term.