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

Freedom and Information

Assessing Publicly Available Data Regarding U.S. Transportation Infrastructure Security

Eric Landree, Christopher Paul, Beth Grill,
Aruna Balakrishnan, Bradley Wilson,
Martin C. Libicki

Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

The research described in this report was conducted under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment (ISE).

Library of Congress Cataloging-in-Publication Data

Landree, Eric.
Freedom and information : assessing publicly available data regarding U.S. transportation infrastructure security / Eric Landree ... [et al.].
p. cm.
Includes bibliographical references.
ISBN-13: 978-0-8330-4031-2 (pbk.)
1. Terrorism—United States—Prevention—Evaluation. 2. Terrorism—Risk assessment—United States. 3. Transportation—Effect of terrorism on—United States. 4. Transportation—Security measures—United States. 5. Infrastructure (Economics)—United States—Safety measures. 6. National security—United States—Planning. I. Title.

HV6432.L363 2004
363.325'93880973—dc22

2006032345

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.

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

This report concerns the feasibility of obtaining information relevant to planning terrorist attacks from publicly available sources. To the extent that such information is available, it is particularly valuable to terrorist planners in that it can generally be obtained at lower cost, risk, and effort than more direct forms of gathering information such as observation of a potential target. Familiarity with public sources of information is also valuable to defenders. If they are unaware that a terrorist group knows or can easily learn about a particular vulnerability, that vulnerability can be exploited more easily. If, however, defenders are able to establish a rough idea of what terrorists are likely to know or can learn from public sources, they can better identify what assets, regions, or populations may be at risk and adjust their defenses accordingly.

Given the vast array of information in the public domain, identifying all the information relevant to a potential target and assessing its potential value to terrorist planners is daunting. What is needed is a way to define the kinds of information most likely to be useful in planning and executing attacks on particular targets. We developed a framework to guide assessments of the availability of such information for planning attacks on the U.S. air, rail, and sea transportation infrastructure, and applied the framework in a red-team information-gathering exercise. Our results demonstrate the utility of the framework for identifying publicly available information relevant to planning terrorist attacks. They also allow us to describe the level of difficulty involved in finding various kinds of information relevant to specified attack scenarios.

Research Approach

Our research approach involved four steps. First, we identified six plausible attack scenarios—two each in airline, rail, and sea transportation infrastructures—against which to assess the accessibility of publicly available information. Second, to guide information gathering relevant to these scenarios and to assess the adequacy of results, we developed the modified intelligence preparation of the battlefield (ModIPB) framework. Based primarily on U.S. Army doctrine regarding intelligence preparation of the battlefield (IPB), this framework specifies four categories of information relevant to targets in the transportation infrastructure, including (1) avenues of approach and ease of access, (2) target features, (3) security (including forces, security measures, and other population groups present), and (4) analysis of threats to the terrorist operation. Third, we designated a "red team" to serve as proxies for terrorists seeking

information about each of the potential attack scenarios. Team members were instructed to find information sufficient to complete an operational plan for each of the six scenarios, relying on the ModIPB framework as a guide and using only very low- or no-risk information-gathering activities—that is, public source, off-site research. Fourth, we undertook three validation exercises to assess the relevance and completeness of the information collected.

Findings

The primary contribution of this research is the observation that the ModIPB framework is useful in directing analyses of publicly available information that would be needed to plan terrorist attacks across a wide variety of transportation infrastructure targets and attack methods; this outcome suggests that the framework is broadly applicable to the problem of identifying information that might reveal vulnerabilities in those systems. In addition, it became evident from applying this framework what types of information are relatively hard versus relatively easy to find for the set of six scenarios describing potential attacks.

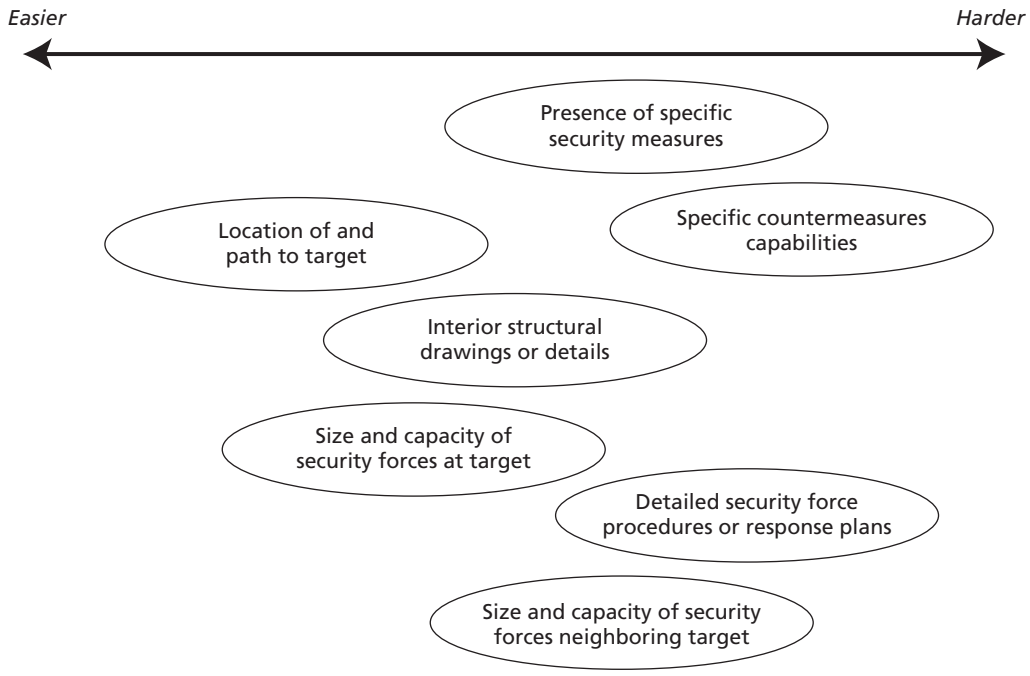
The ModIPB framework is a useful guide to locating information relevant to the planning and execution of terrorist attacks. A detailed presentation of all the results—that is, the kinds of information that the red team did and did not find for each scenario—appears in Appendix A. As a whole, our findings demonstrate that the ModIPB framework performed well as a guide to helping red-team members locate information relevant to the attack. Relying on the checklists we provided, red-team members were able to identify information that, with scattered exceptions, proved useful for planning the hypothetical terrorist attacks across all six scenarios. This assertion is supported by the results of three validation exercises.

Ease of identifying relevant information varied across information categories, with general descriptive information being easiest to find and information concerning detailed security procedures being most difficult to find. Information is considered "easy to find" if, as determined by the red-team exercise, the same type of information is available from multiple sources for multiple infrastructure targets of a similar type (e.g., all airports). Information is considered "hard to find" if only single examples were located or if no information was located. Some types of information could be found for one class of infrastructure or for one scenario, but not others.

Given this variation and the relatively small number of scenarios we studied, we cannot compare the ease of finding information across categories with great precision, but our findings do suggest that certain categories of information are generally easier to find than others. Members of the red team found information concerning the location of terrorist targets, interior structural details, and the size and capacity of security forces relatively easily, but locating information concerning specific security procedures and capabilities was more difficult. A notional summary of the findings is shown in Figure S.1.

For each of the attack scenarios, the red team was unable to locate some of the information that a terrorist planner would need to assess the likely success of a potential attack. For example, for some scenarios, the team found news articles reporting the number of officers that monitor a particular area, but those reports did not provide detailed information about

Figure S.1
Notional Representation of Information Collected by Red Team



operational plans or deployments at specific stations. That is, the information regarding operational plans and security force deployments was "hard to find."

Policy Recommendations

First, we note that, regardless of how easy or hard it was to locate certain information, there is no evidence from this investigation to suggest that removing information from the public domain would alter the risk of a given scenario occurring. Our findings concern only how easily the red team was able to locate relevant information.

Based on the findings described above, we propose two recommendations intended to help infrastructure owners increase security.

- **To prevent information that includes security details from entering the public domain, review and revise procedures for operational and information security.** Our findings indicate that information pertaining to certain ModIPB categories is not easily accessible through off-site, public information sources. For example, information concerning security force deployments—that is, routes, schedules, number of personnel, vehicles patrolling—is not easily accessible through off-site, public information sources. Nonetheless, our red team did identify a wide variety of kinds of information concerning the air, rail, and sea transportation infrastructures, including overhead images, schemat-

ics of sites and equipment, and news reports. Moreover, new information is being added to the public domain every day, along with new capabilities for searching and fusing information. Thus, procedures for securing sensitive information should be evaluated regularly, taking into account developments in technologies for storing and retrieving data, with a view toward identifying vulnerabilities that might allow sensitive information to enter the public domain.

- **Include information that can be obtained from easily accessible, off-site public information sources in vulnerability assessments.** The operations of transportation infrastructure organizations have proven to be attractive targets for terrorist attacks. Thus the owners and operators of these facilities must—and do—conduct vulnerability assessments to identify threats to the security of their assets and activities. To ensure the comprehensiveness of these assessments, information that is appropriately in the public domain must be included.

  Our results indicate that the utility and comprehensiveness of information available in the public domain varies by infrastructure and scenario. Given this variation, owners and operators of transportation infrastructure organizations must focus particularly on how information available in the public domain is likely to affect the vulnerability of the specific assets and activities of their own organizations. Relying on ModIPB framework as a tool to guide information searches will help these organizations identify such information, which can then be included in vulnerability assessments.

  Owners and operators of transportation infrastructure organizations must determine how frequently vulnerability assessments should be conducted to ensure that, as new information enters the public domain, it is captured in those assessments. Because such new information can enter the public domain at any time, including the day after a vulnerability assessment is conducted, we cannot specify a priori how frequently such reviews should be conducted. We believe, however, that analyses of information in the public domain should either be integrated into current vulnerability assessments or, if conducted separately, should be carried out with at least the same frequency.