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

Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection

Henry H. Willis, Tom LaTourrette, Terrence K. Kelly, Scot Hickey, Samuel Neill

Prepared for the Department of Homeland Security

CENTER FOR TERRORISM RISK MANAGEMENT POLICY

The research described in this report was conducted by the RAND Center for Terrorism Risk Management Policy for the Department of Homeland Security.

Library of Congress Cataloging-in-Publication Data

Terrorism risk modeling for intelligence analysis and infrastructure protection / Henry H. Willis ... [et al.].
p. cm.
Includes bibliographical references.
ISBN-13: 978-0-8330-3974-3 (pbk. : alk. paper)
1. Terrorism—Risk assessment—United States. 2. Cities and towns—United States. 3. Terrorism—United States—Prevention. 4. Terrorism—Prevention—Research. I. Willis, Henry H.

HV6432.T469 2006
363.32501'1—dc22

2006018380

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
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

When are terrorists likeliest to attack next? Will they use chemical, biological, radiological, or nuclear (CBRN) weapons or resort to sabotage or conventional attacks? What locations or facilities will they target? What economic impact would a conventional attack on a piece of critical infrastructure have in comparison with a nuclear attack? The Office of Intelligence and Analysis (OI&A)[1] at the Department of Homeland Security is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the United States.

Recognizing that there are not enough available resources to reduce all risks, DHS has adopted a focused approach. DHS is moving increasingly to risk analysis and risk-based resource allocation, a process that is designed to manage the greatest risks instead of attempting to protect everything. Efforts to develop analytical tools necessary to support this approach and institutionalize their use across the department are just beginning. In this context, OI&A is exploring how existing risk-analysis tools might be useful for its Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). This report presents the results of three applications of a model routinely used by the insurance industry to assess liability from terrorism risk: the Probabilistic Terrorism Model developed by Risk Management Solutions, Inc. (RMS). Informative and useful findings were taken as a positive indication that the model would be a valuable resource for HITRAC.

As part of CTRMP, RMS (along with other private sector organizations) funds research on terrorism risks and provides RAND with access to the RMS Probabilistic Terrorism Model for research purposes. This report applies the RMS Probabilistic Terrorism Model to compare terrorism risks across different urban areas, to assess terrorism risks within a metropolitan area, and to target intelligence analysis. The RMS model is broadly applied in the insurance industry and therefore represents a relevant example for study of how insurance-industry models can be used by DHS.

The RMS model estimates the risks of macroterrorism, which RMS defines as attacks capable of causing (1) more than $1 billion in economic losses, (2) more than 100 fatalities or 500 injuries, or (3) massively symbolic damage. Starting with specific attack scenarios, the model assesses the threat of various types of attack on different targets, the vulnerability of

[1] OI&A was formerly the Office of Information Analysis in the Information Analysis and Infrastructure Protection Directorate (IAIP).

those targets to those attacks, and the expected annual consequences of successful attacks in terms of casualties and property loss. The overall risk of any given attack scenario reflects all three of these factors.

The first application shows how terrorism risk modeling can be used to support resource allocation decisions required in programs such as the DHS Urban Area Security Initiative (UASI). The second application demonstrates how the model could be used to develop standard profiles of terrorism risk in specific cities, which, while useful as part of a nationwide profiling effort for DHS, could be particularly valuable for distribution to the appropriate state and local governments. The third application suggests that the RMS model could be used as part of an intelligence-analysis tool for helping OI&A translate information about goals and capabilities of terrorist cells into advice for local law enforcement and the intelligence community on how to target surveillance efforts.

Using Risk Management Solutions to Assess Risk Across Cities

The first application used the RMS model to compare terrorism risk across metropolitan areas that received funding from the UASI grant program in 2005. The fundamental conclusion of this analysis is that, according to the RMS model, terrorism risk is concentrated in a small number of those designated UASI cities, with most cities having negligible relative risk. For example, considering fatalities only, New York accounts for 65 percent of the national risk, with the next closest city, Chicago, having 12 percent. After Chicago, risk to other individual cities falls off steeply. The top eight cities account for more than 95 percent of the nation's risk from terror attacks. Furthermore, the estimated proportion of terrorism risk in each urban area exceeded the share of population and the actual UASI allocation percentages in only three urban areas: New York, Chicago, and San Francisco. These results do not change significantly when considering property loss.

There is some variability in how RMS estimates of terrorism risk are distributed across cities when considering conventional, CBRN, and sabotage attacks separately. Those few cities that do experience substantial changes with regard to CBRN do so for readily apparent reasons. For example, estimates of the proportion of terrorism risk in Jersey City, New Jersey, are significantly higher for CBRN risk, but this appears to be due to its proximity to New York City, with its comparatively high risk of CBRN attacks. Estimates of sabotage risk are highly dependent on proximity of nuclear power plants, chemical plants, or oil refineries to each city. Cities without major facilities of these types are not estimated to be significantly exposed to sabotage attacks.

This analysis highlights the value of considering different perspectives on risk. While this study has assessed only terrorism risk, DHS is also responsible for managing risks of natural disasters. Similar insurance-industry models of natural disaster risk could be readily incorporated into this type of analysis.

This application also points to several paths to making insurance-industry models such as the RMS model more useful for resource allocation decisionmaking. First, the model databases, particularly the target database, should be compared to other data sets and possibly

expanded. Second, the consequence model should be linked to other models of indirect economic impacts to understand the relative importance of the consequences of interconnected infrastructure systems. Third, the results of this analysis should be compared to analyses using different assumptions about terrorist threats and different models, including those that address natural disaster risk. Finally, results such as these should be incorporated into further analysis of how to connect resource allocation to risk reduction and debates about U.S. tolerance of terrorism risk.

This application resulted in the following recommendations:

- DHS should incorporate terrorism estimates such as these, along with natural disaster risk estimates, into the assessment process to support grant allocations and other assistance to states and localities.
- DHS should consider investing in the extensions of insurance-industry models noted previously to improve the usefulness of this approach to homeland security analyses.

Using the RMS Model to Assess Risk Within Specific Cities

As an example of intracity analysis, we presented an assessment of the terrorist threat in Las Vegas using the RMS model. This analysis helps answer three questions:

1. How does the overall terrorism risk in Las Vegas compare to that in other cities?
2. How do potential terrorist attack targets within Las Vegas rank in terms of overall risk and three constituent components of risk: threat, vulnerability, and consequence?
3. How does the risk ranking change when examining particular attack modes or when considering available intelligence?

Answering questions regarding attack mode likelihood provides local homeland security officials with information concerning the types of attack for which they should prepare. The attractiveness to terrorists of particular attack modes depends partially on available targets and other local characteristics that vary from one city to another. Information on consequences gives local officials an understanding of what the effects of such attacks might be and what resources might be required to respond. Finally, information on risk provides local, state, and federal homeland security leaders with the basis for understanding the trade-offs between the probability of an attack and its consequences as well as a metric (i.e., expected fatalities or property losses) for making decisions on prevention and protection actions. This assessment of risk can be quickly readjusted to account for new intelligence about likely attacks of a specific kind (e.g., on Las Vegas hotels or casinos). Thus the RMS model can be used to evaluate how the relative risk might change in Las Vegas as a function of new information.

In general, this analysis provided a city profile with distinct risk characteristics that could be used to help inform and guide prevention and protection activities. Similar city profiles for

other major cities could help inform DHS grant and other programs for prevention, protection, response, and recovery.

The analysis also provides insights into potential model extensions. One important capability of the RMS model is the ability to reflect how features of individual targets affect the likelihood or consequences of a terrorist attack. In the model, individual targets are assigned an iconic value, which affects the calculation of likelihood that the target will be attacked. In addition, the model can account for different levels of security, both visible and invisible, that could act as deterrents to or mitigate the consequences of terrorist attacks. Generally, however, these model capabilities are underutilized, because the specific information needed to assess these parameters for individual buildings is not available. Collecting and incorporating such data for specific localities or industry sectors would enhance the utility of the model.

The RMS model also excludes casualties for some target types. In most cases, the model accounts for people in only three places: at work, at home, or in school. As a result, modeled casualties do not include hotel and casino guests or visitors, nor do they account for passersby on the street. In addition, because the model is designed for insurance purposes, government buildings (and employees), which are generally not covered by the insurance industry, are also not captured. These are issues in the model that need to be addressed to improve its utility for assisting DHS as well as state and local governments in their missions. Assuming that additional data of these types are available, accommodating them in the model will be straightforward

Analysis of the second application resulted in the following recommendations:

- DHS should work closely with state and local homeland security officials in major metropolitan areas to familiarize them with this approach to analyzing the threats and consequences of attacks and city-specific risk measures that may be indicated.
- DHS should consider funding the development of city profiles, similar to that done in this analysis for Las Vegas, and working with state and local officials to develop city risk profiles for major metropolitan areas receiving DHS preparedness grants.

Using Risk Management Solutions to Assist Intelligence Analysis

In the third application, we incorporated the RMS model into the process typically used by OI&A analysts for analyzing raw intelligence to identify likely targets and attack modes in the United States. OI&A uses this process to provide local law enforcement around the country with "actionable intelligence": guidance about whom and what to look for, where, and when. The goal was to see what attack modes the RMS model indicates corresponding to knowledge from raw intelligence of suspected terrorist groups' capabilities and intentions.

This approach seeks to do two things. First, it identifies the specific targets and attack modes of greatest risk that meet terrorist goals. Doing so relies on the ability to translate terrorist goals and intentions into specific levels of fatalities, injuries, or damages to allow discrimination among targets in the risk-analysis model. Second, it compares the attack types with assessments from the intelligence community of terrorist capabilities. This may eliminate

those scenarios that are beyond the capabilities of the terrorist group in question. The result of this approach is a list of terrorism scenarios that both fulfill a terrorist group's goals and are within their capabilities, as determined by the intelligence community. The primary limitation of this process is that the output represents only those attack mode target pairs resident in the RMS model. Thus, while it could help focus analysis, it is vulnerable to ignoring scenarios that involve new targets or attack modes.

This methodology could be made more useful by refining the output of the process in three ways. First, a process could be developed for translating general statements about terrorist group motivations into desired consequences and associated attack types using metrics consistent with the RMS model. Second, using information about the anticipated timelines, material requirements, and skill levels required for specific terrorist attacks, specific indicators of the identified attack modes in identified locations could be generated to give law enforcement actionable items for which to look. Third, tabletop exercises could be developed to test this method, provide feedback, and refine the concept and model.

These activities are well within the realm of the possible but require resources and interaction between and among a competent research staff, the intelligence community, and the law enforcement community. Analysis of this application resulted in the following recommendations:

- DHS should develop a methodology for translating general intelligence on terrorists' capabilities and intentions into metrics consistent with metrics used in models like the RMS model (i.e., deaths, injuries, and property damage).
- DHS should also develop descriptions of terrorist attack planning and operations that can be used to translate estimates from risk models of likely attack scenarios into detailed recommendations of what law enforcement should be looking for to prevent specific types of attack based on intelligence information.
- DHS should develop tabletop exercises and use them to test the process and provide feedback that would lead to improvements in the use of this model.