



# CENTER FOR TERRORISM RISK MANAGEMENT POLICY

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](http://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](http://www.rand.org)

Explore [RAND Center for Terrorism Risk Management](#)

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  
R E P O R T

---



# 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.

© 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  
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](mailto:order@rand.org)

## Preface

---

The Office of Intelligence and Analysis 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 is moving to greater use of 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, the Office of Intelligence and Analysis is exploring how existing risk-analysis tools might be useful for its Homeland Infrastructure Threat and Risk Analysis Center. 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).

As part of RAND's Center for Terrorism Risk Management Policy (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 and collection efforts. 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. These findings should be of interest to those at all levels of government and in the private sector responsible for analyzing intelligence information, allocating resources, and developing strategic and tactical responses to protect the United States from terrorist threats.

This is one of a series of reports that CTRMP has published on terrorism risk assessment. Readers may also be interested in *Estimating Terrorism Risk* (Willis et al., 2005).

### **The RAND Center for Terrorism Risk Management Policy**

CTRMP provides research that is needed to inform public and private decisionmakers on economic security in the face of the threat of terrorism. Terrorism risk insurance studies provide the backbone of data and analysis to inform appropriate choices with respect to government involvement in the market for terrorism insurance. Research on the economics of various

liability decisions informs the policy decisions of the U.S. Congress and the opinions of state and federal judges. Studies of compensation help Congress to ensure that appropriate compensation is made to the victims of terrorist attacks. Research on security helps to protect critical infrastructure and to improve collective security in rational and cost-effective ways.

CTRMP is housed at the RAND Corporation, an international nonprofit research organization with a reputation for rigorous and objective analysis and the world's leading provider of research on terrorism. The center combines three organizations:

- RAND Institute for Civil Justice, which brings a 25-year history of empirical research on liability and compensation
- RAND Infrastructure, Safety, and Environment, which conducts research on homeland security and public safety
- Risk Management Solutions, the world's leading provider of models and services for catastrophe risk management.

For additional information about the Center for Terrorism Risk Management Policy, contact

Robert Reville  
RAND Corporation  
1776 Main Street  
P.O. Box 2138  
Santa Monica, CA 90407  
Robert\_Reville@rand.org  
310-393-0411, x6786

Michael Wermuth  
RAND Corporation  
1200 South Hayes Street  
Arlington, VA 22202  
Michael\_Wermuth@rand.org  
703-413-1100, x5414

A profile of CTRMP, abstracts of its publications, and ordering information can be found at <http://www.rand.org/multi/ctrmp/>.

## Center for Terrorism Risk Management Policy Advisory Board

---

**Jeffrey D. DeBoer (Cochair)**

President and chief executive officer  
Real Estate Roundtable

**Jack Armstrong**

Assistant vice president  
Senior regulatory counsel  
Liberty Mutual Insurance Company

**Andrew Coburn**

Vice president of catastrophe research  
Director of terrorism research  
Risk Management Solutions, Inc.

**Ken Jenkins**

Chief underwriting officer  
American Reinsurance RiskPartners

**Kathleen Nelson**

Immediate past chair  
International Council of Shopping Centers

**Kevin Scroggin**

General director  
Corporate Risk Management and Insurance  
General Motors

**Cosette Simon**

Senior vice president  
Swiss Re Life and Health America Inc.

**Steven Wechsler**

President and chief executive officer  
National Association of Real Estate Investment  
Trusts

**Pierre L. Ozendo (Cochair)**

Member of the executive board  
Head of Americas Property and Casualty  
Swiss Re America Holding Corporation

**Brian Boyden**

Executive vice president  
State Farm Insurance

**Kenneth Feinberg**

Managing Partner  
The Feinberg Group, LLP

**Peter Lowy**

Chief executive officer  
Westfield Corporation, Inc.

**Art Raschbaum**

Executive vice president  
Managing director  
GMAC RE

**Hemant Shah**

President and chief executive officer  
Risk Management Solutions, Inc.

**Richard Thomas**

Senior vice president  
Chief underwriting officer  
American International Group





# Contents

---

<b>Preface</b> .....	iii
<b>Center for Terrorism Risk Management Policy Advisory Board</b> .....	v
<b>Figures</b> .....	ix
<b>Tables</b> .....	xi
<b>Summary</b> .....	xiii
<b>Acknowledgments</b> .....	xix
<b>Abbreviations</b> .....	xxi

## CHAPTER ONE

### **Terrorism Risk Models for the Insurance Industry:**

<b>A New Resource for Intelligence Analysts</b> .....	1
Risk Analysis Can Help OI&A Focus Its Analysis and Prioritize Resources .....	1
Leveraging Risk-Analysis Tools from the Insurance Industry .....	2
Adapting the RMS Model for Use by DHS .....	3
Structure of the Report .....	3

## CHAPTER TWO

### **Terrorism Risk Modeling for the Insurance Industry:**

<b>The RMS Probabilistic Terrorism Model</b> .....	5
Modeling Terrorist Threats as Probability of Attack .....	6
Estimating City Tier Likelihood .....	7
Estimating Target Type and Individual Target Likelihoods .....	8
Estimating Attack Mode Likelihood .....	9
Estimating Relative Attack Likelihood .....	10
Estimating Overall Attack Likelihood .....	12
Modeling Attack Consequences .....	12
Applicability of the RMS Model to DHS Decisionmaking .....	13

## CHAPTER THREE

<b>Application 1: Terrorism Risk in UASI Areas</b> .....	15
Methodology .....	16
Results of Analysis .....	18
How Is Terrorism Risk Distributed Across UASI Cities? .....	18

Is the Distribution of RMS Terrorism Risk Estimates Different When Measured as Property Risk Versus Fatality Risk? .....	20
How Does the Distribution of RMS Risk Estimates Differ by Attack Mode? .....	20
Conclusions About Risk and Observations About the Model .....	27

#### CHAPTER FOUR

<b>Application 2: Profiling Terrorism Risk in Las Vegas</b> .....	29
Attack Probabilities in Las Vegas .....	29
Consequences of Terrorist Attacks in Las Vegas .....	30
Terrorist Attack Risk in Las Vegas .....	36
Variation in Risk by Target Type .....	36
Variation in Risk by Attack Type .....	38
Variation in Risk by Consequence Measure .....	39
Spatial Variations in Risk .....	39
Using Intelligence to Constrain Risk Estimates .....	40
Effect on Risk of Increased Probability of Attacks on Hotel-Casinos .....	42
Summary and Conclusions .....	43

#### CHAPTER FIVE

<b>Application 3: Informing Threat Assessment Using the RMS Terrorism Risk Model</b> .....	45
Overview of Approach .....	45
Can Intentions Be Matched with Outcomes? .....	47
Options for Refining This Analytic Approach .....	48

#### CHAPTER SIX

<b>Conclusions and Recommendations</b> .....	51
Using Terrorism Models to Assess Risk Across Cities .....	51
Recommendations .....	53
Using Terrorism Models to Assess Risk Within Specific Cities .....	53
Recommendations .....	55
Using Terrorism Risk Models to Assist Intelligence Analysis .....	55
Recommendations .....	56

#### APPENDIXES

<b>A. RMS Terrorism Advisors' Network</b> .....	57
<b>B. City Tiers and Likelihoods from the RMS Probabilistic Terrorism Model</b> .....	59
<b>C. Definitions of Fiscal Year 2005 UASI-Eligible Urban Areas</b> .....	61
<b>D. Example of Filtering Risk-Analysis Results Using Intelligence Assessments of Terrorist Capabilities</b> .....	65

<b>References</b> .....	71
-------------------------	----

## Figures

---

2.1.	Logic and Structure of Modeling Terrorism Risk .....	6
2.2.	Relative Likelihood of Terrorist Attack in Different City Tiers.....	8
2.3.	Relative Likelihood of Terrorist Attack for Different Attack Modes .....	11
2.4.	Overall Relative Attack Likelihood for Different Cities .....	12
3.1.	RMS Probabilistic Terrorism Model Estimates for the Fraction of Total Risk for Each of the Urban Areas Eligible for UASI Funding in 2005, Considering All Attack Modes.....	19
3.2.	Comparison of RMS Probabilistic Terrorism Model Estimates for the Fraction of Total Risk for Each of the Urban Areas Eligible for UASI Funding in 2005 in Fatalities Versus in Property Losses, Considering All Attack Modes.....	21
3.3.	Comparison of RMS Probabilistic Terrorism Model Estimates for the Fraction of Total Risk for Each of the Urban Areas Eligible for UASI Funding in 2005, Considering All Attack Modes Versus Conventional Attack Modes Only .....	22
3.4.	Comparison of RMS Probabilistic Terrorism Model Estimates for the Fraction of Total Risk for Each of the Urban Areas Eligible for UASI Funding in 2005, Considering All Attack Modes Versus Chemical, Biological, Radiological, or Nuclear Attack Modes Only .....	23
3.5.	Comparison of RMS Probabilistic Terrorism Model Estimates for the Fraction of Total Risk for Each of the Urban Areas Eligible for UASI Funding in 2005, Considering All Attack Modes Versus Sabotage Attack Modes Only.....	24
3.6.	Percentage of Terrorism Risk for Each of the Urban Areas Eligible for UASI Funding in 2005 by Category of Attack Mode .....	26
4.1.	Distribution of Targets by Group in Las Vegas and the Entire Country .....	30
4.2.	Fatality Estimates for a 600-lb Bomb Attack on Targets in Las Vegas.....	32
4.3.	Property Loss Estimates for a 600-lb Bomb Attack on Targets in Las Vegas .....	33
4.4.	Fatality Estimates for a 1-Ton Bomb Attack on Targets in Las Vegas.....	34
4.5.	Property Loss Estimates for a 1-Ton Bomb Attack on Targets in Las Vegas .....	35
4.6.	Framework for Examining Terrorist Attack Risk.....	36
4.7.	Fatality Risk for Terrorist Attacks on Different Target Types in Las Vegas .....	37
4.8.	Fatality Risk for Terrorist Attacks Using Different Attack Modes at Hotel-Casinos.....	38
4.9.	Property Loss Risk for Terrorist Attacks on Different Target Types in Las Vegas.....	39
4.10.	Distribution of Average Annual Loss of Property in Las Vegas.....	40
4.11.	Fatality Risk for Terrorist Attacks in Las Vegas for a Limited Selection of Attacks .....	42
4.12.	Risk Profile for Terrorist Attacks in Las Vegas for a Limited Selection of Attack Modes and Hotel-Casinos Raised to Target Type Tier 1 .....	43
5.1.	Approach for Incorporating Risk-Analysis Tools into the Intelligence Process .....	46

D.1. Relationship Between Logistics Burden and Attack Type.....69

## Tables

---

2.1.	RMS Target Type Groups .....	9
2.2.	Modes of Attack Modeled in the RMS Terrorism Risk Model .....	10
3.1.	Homeland Security Council National Planning Scenarios and Comparable RMS Scenarios .....	17
4.1.	Logistics Capability Estimates for Past Hotel Attacks .....	41
B.1.	City Tiers and Likelihoods from the RMS Probabilistic Terrorism Model .....	59
C.1.	Definitions of Fiscal Year 2005 UASI-Eligible Urban Areas .....	61
D.1.	Logistics Capabilities Implied by NYPD Case Studies .....	66
D.2.	Attack Modes That Terrorist Groups Involved in the USS <i>Cole</i> and Bali Bombing Terrorist Events Could Execute Based on Filtering of the RMS Model Using Assessments Made in NYPD Case Studies .....	67
D.3.	Sensitivity Analysis of Importance of Time and Financial Resources for Attack Mode Capabilities of 1993 Landmark Plot Terrorists .....	68



## 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)<sup>1</sup> 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

---

<sup>1</sup> 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.



## Acknowledgments

---

We would like to thank all those who contributed to this report through their comments, support, and dedication. Throughout the project, Glenn Coplon, John MacLaren, Bob Ross, Melissa Smislova, Susan Smith, Paul Speller, John Sturgeon, and David Weinberg at DHS provided critical feedback to help the direction of this research. RMS provided access to the RMS Probabilistic Terrorism Model, and Derek Blum, Alie Cohen, Andrew Coburn, and Peter Ulrich of RMS helped us ensure that we drew proper conclusions from our analysis. Our RAND colleague, Craig Martin, generously shared his experience with analysis using the RMS model. We thank Robert Reville, Michael Wermuth, and the entire board of CTRMP for their comments on early drafts of this document. We also thank Lisa Sheldone and Alissa Hiraga for the dedication and attention to detail that they brought to the production of this report. Needless to say, any errors or omissions in the book are the sole responsibility of the authors.



## Abbreviations

---

AAL	average annual loss
CBRN	chemical, biological, radiological, or nuclear
CTRMP	Center for Terrorism Risk Management Policy
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSC	Homeland Security Council
IAIP	Information Analysis and Infrastructure Protection Directorate
NIPP	National Infrastructure Protection Plan
NYPD	New York City Police Department
OI&A	Office of Intelligence and Analysis
RMS	Risk Management Solutions
TRIA	Terrorism Risk Insurance Act of 2002
UASI	Urban Area Security Initiative





## **Terrorism Risk Models for the Insurance Industry: A New Resource for Intelligence Analysts**

---

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 and 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)<sup>1</sup> at DHS is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the United States. This report documents the results of analysis using a risk-analysis tool, the Risk Management Solutions (RMS) Probabilistic Terrorism Model, to help OI&A with this challenge.

### **Risk Analysis Can Help OI&A Focus Its Analysis and Prioritize Resources**

Recognizing that there are not enough available resources to reduce all risks, DHS has adopted a more focused approach. DHS is moving to greater use of 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 it might use existing risk-analysis tools to identify what types of information to collect and how to interpret it. OI&A, in particular, is interested in investigating the possible uses of risk-analysis tools, because the information the tools can generate is directly related to the types of questions OI&A is called on to answer—questions involving the likelihood and consequences of possible attacks.

Calculating the risk of a terrorist attack against a certain target involves assessing, first, whether or not a threat exists; second, whether that target is vulnerable; and third, what damage would result if the attack were successfully carried out. The first two of these factors—threat and vulnerability—have to do with the likelihood that a certain attack will occur. The third, the type and magnitude of resulting damage, comprises the consequences. Taken as a whole,

---

<sup>1</sup> OI&A was formerly the Office of Information Analysis in the Information Analysis and Infrastructure Protection Directorate (IAIP).

these three assessments indicate the overall level of risk for a specific attack on a given target (Willis et al., 2005).

Analyzing risk in this way has several important benefits. All three factors that contribute to specific terrorism risks are uncertain. Risk analysis increases transparency of risk estimates by helping decisionmakers to better understand which of the factors contribute to specific terrorism risks and which are of greatest importance in specific scenarios. For example, some scenarios may involve likely events (i.e., high threat) with moderate to low consequences, and others may involve high-consequence but low perceived likelihood events. Risk analysis also provides a framework for managing risk by enabling analysts to contrast different potential events using common measures, for example, people injured or property damage incurred.

### **Leveraging Risk-Analysis Tools from the Insurance Industry**

Since 2001, companies in the insurance industry have begun using terrorism risk models to help understand and manage their exposure to terrorism losses in different markets. As part of DHS's learning process, OI&A asked the RAND Corporation to explore how these tools might be useful for its Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). HITRAC provides intelligence analysis about terrorism threats in the United States and risk assessments to help protect critical infrastructure.

One such insurance-industry model is the Probabilistic Terrorism Model developed by RMS (RMS, undated). Founded at Stanford University in 1988, RMS provides the insurance and reinsurance industries with products and services for quantifying and managing catastrophe risks. The RMS model estimates the risk 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 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.<sup>2</sup>

RMS is a founding sponsor of the RAND Center for Terrorism Risk Management Policy (CTRMP). Because of its affiliation with RAND, the company gives RAND access to the Probabilistic Terrorism Model to support public policy analysis, such as this work for OI&A. The RMS model is broadly applied in the insurance industry and therefore represents a relevant example for the study of how insurance-industry models can be used by DHS. To assess its utility in the context of homeland security policy, we used it in three applications relevant to DHS's needs. Informative and useful findings were taken as a positive indication that the model would be a valuable resource for HITRAC. The findings generated by each application are good examples of the strengths and limitations of tools developed for the insurance industry for problems relevant to DHS.

---

<sup>2</sup> Two other firms, Equecat, Inc. and AIR Worldwide, Inc., each have developed their own terrorism risk models to support the insurance and reinsurance industries. These models are conceptually similar to the RMS model.

In the first application, we used the model in the context of DHS's Urban Area Security Initiative (UASI). This is a grant program through which DHS provides funds to urban areas to improve emergency preparedness. By law, this program is required to distribute funds according to risk. We applied the model to estimate how risk is distributed across major metropolitan areas in the United States that had received UASI program funds in 2005.

In the second application, we used the model to understand the distribution and nature of terrorism risk within a specific city: Las Vegas. This demonstrated 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.

In the third application, we incorporated the RMS model into the process typically used by OI&A analysts to analyze 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.

## **Adapting the RMS Model for Use by DHS**

Recognizing that DHS has different needs from users in the insurance industry, our secondary purpose in conducting this study was to evaluate the existing RMS model for use by OI&A. In this context, we set out to identify those features of the current design well suited to OI&A's needs as well as its limitations in that regard. In running the three applications, we were able to make meta-observations about where the model seems most helpful and where it can be extended to increase its utility for OI&A, for example, by adding information to the model's database, incorporating more or different threat scenarios, or assessing a broader range of consequences.

## **Structure of the Report**

Chapter Two provides an overview of the RMS Probabilistic Terrorism Model. Chapter Three presents Application 1, "Terrorism Risk in UASI Areas." Chapter Four presents Application 2, "Profiling Terrorism Risk in Las Vegas." Chapter Five presents Application 3, "Informing Threat Assessment Using the RMS Terrorism Risk Model." Chapter Six provides an overview of conclusions drawn from these three applications and recommendations for how to extend the RMS model to help it contribute more effectively to DHS's information and analysis needs.



## Terrorism Risk Modeling for the Insurance Industry: The RMS Probabilistic Terrorism Model

---

The attacks of September 11, 2001, were unprecedented. Never before had terrorist attacks killed thousands and destroyed billions of dollars in property. This was a new risk for the insurance industry, and the immediate response indicated that it was too poorly understood to be managed. Shortly after the attacks, reinsurers and primary insurers stopped covering terrorism losses (Dixon et al., 2004). With the passage of the Terrorism Risk Insurance Act (TRIA) in November of 2002, the insurance industry was required to offer coverage for terrorism losses and thus needed to better understand exposure to this risk. For help, the industry looked to catastrophe modeling.

Catastrophe modeling is used to assess the likelihood that disasters will occur, the potential consequences if they occur, and the distribution of the absolute and relative risk in different places and at different times. It has been successfully applied to study the risks of hurricanes, earthquakes, floods, and wind damage. After September 11, 2001, several firms with expertise in modeling catastrophes began modeling terrorism losses.<sup>1</sup> These models are used by the insurance industry to assess the possible losses in a specific area where insurance policies may be held or from attacks on properties that may be insured.

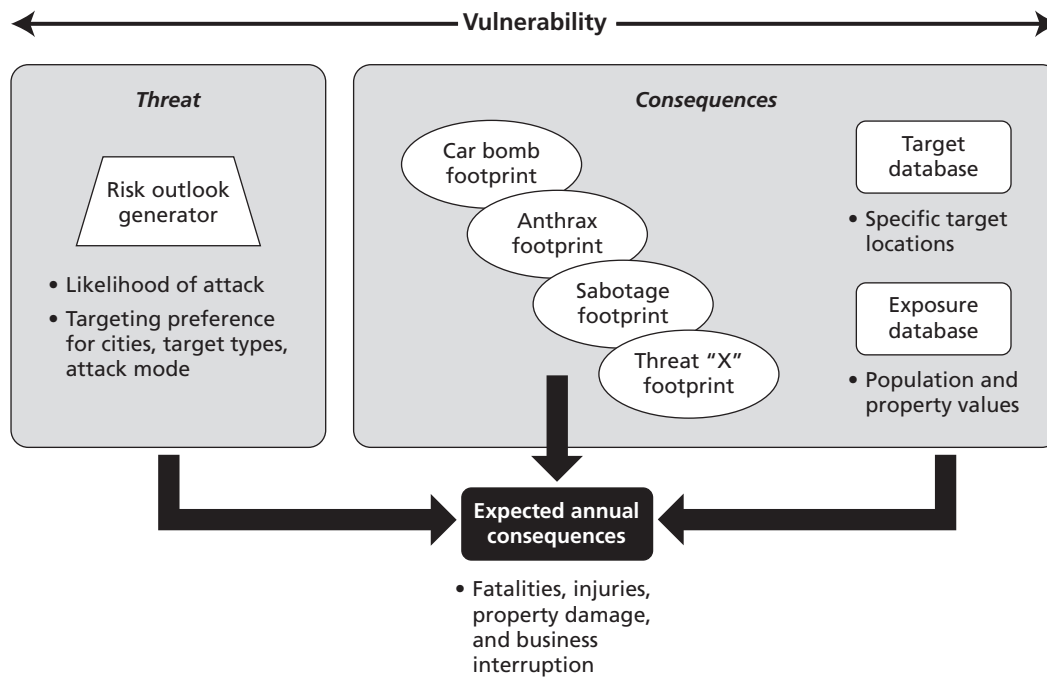
Figure 2.1 depicts the fundamental structure and logic behind many terrorism risk models used by the insurance industry. To reflect risk as a function of threat, vulnerability, and consequence, the models are used to estimate the expected annual human and economic consequences from diverse terrorist threats. The terrorism risk models rely on estimates of the likelihood of different types of attack on different targets based on expert judgment about target selection by terrorists,<sup>2</sup> capabilities for different attack modes, overall likelihood of attack, and propensity to stage multiple, coordinated attacks. The models include vulnerability by reflecting how threats differ from one target to the next based, in part, on how likely attacks on the target are

---

<sup>1</sup> The three most prominent catastrophe modeling firms that developed terrorism risk models are, in alphabetical order, AIR Worldwide, Inc., Equecat, Inc., and Risk Management Solutions, Inc.

<sup>2</sup> Some believe that terrorism threat should not be discussed in terms of probability because historical data do not exist with which to perform actuarial calculations of event frequencies. Bayesian decision theory offers an alternative to the constraints of this frequentist perspective. The Bayesian view is useful for informing decisions when existing information is vague or uncertain yet may lead experts to have a prior belief of probabilities that can later be updated as new information becomes available. Bayesian decision theory allows for incorporation of subjective probability judgments into assessments that may include frequentist calculations. We have adopted a Bayesian perspective on threat likelihood in this report.

**Figure 2.1**  
**Logic and Structure of Modeling Terrorism Risk**



RAND TR386-2.1

to be successful. Vulnerability is also reflected in how the damage profile of different attack modes changes from one target to the next because of target characteristics. Consequences are estimated from modeling of weapon effects and geocoded databases of structural characteristics of targets, population densities, human activity patterns, business activities, and values of buildings and their contents.

All parts of these calculations incorporate assumptions. When using such models, it is important to understand where assumptions are incorporated and how they affect the model calculations. The remainder of this chapter provides an overview of the RMS model structure and assumptions but is not a replacement for a detailed user's manual for the RMS model. Discussion of specific parameter values used in the model is considered proprietary and has been excluded from this description. Additional information on the RMS model can be obtained from the RMS company Web site (RMS, undated) or by contacting RMS directly.

## Modeling Terrorist Threats as Probability of Attack

Terrorist events have fortunately occurred infrequently as compared to accidents and natural disasters. This makes it difficult to look at the historical patterns of terrorism in an effort to guide homeland security policy. In lieu of frequency-based estimates of probability of events occurring, risk analysis has developed a means of determining the probabilities of events occurring by using subjective judgments by experts (Morgan, Henrion, and Small, 1990).

To estimate terrorism threat, the RMS model relies on expert judgments of several factors that could influence a terrorist's affinity to attack specific targets using certain attack modes. These factors can be classified into four components:

- the relative likelihood that any particular city will be attacked
- the relative likelihood that any particular target type will be attacked
- the relative likelihood that any specific target will be attacked because of its inherent iconic value or security
- the relative likelihood that any particular attack mode will be used in an attack.

The relative likelihoods define the probability that, if an attack happens, it will be of a certain type, in a certain place, or on a certain target type.

Expert judgment is also required to assess the absolute probability of attack. RMS classifies this issue into three components:

- the probability that a terrorist attack of any kind will occur in the next year
- the probability that, if an attack occurs, it will be a single attack or a set of coordinated attacks
- the probability that, if an attack occurs, there will be other attacks within the year.

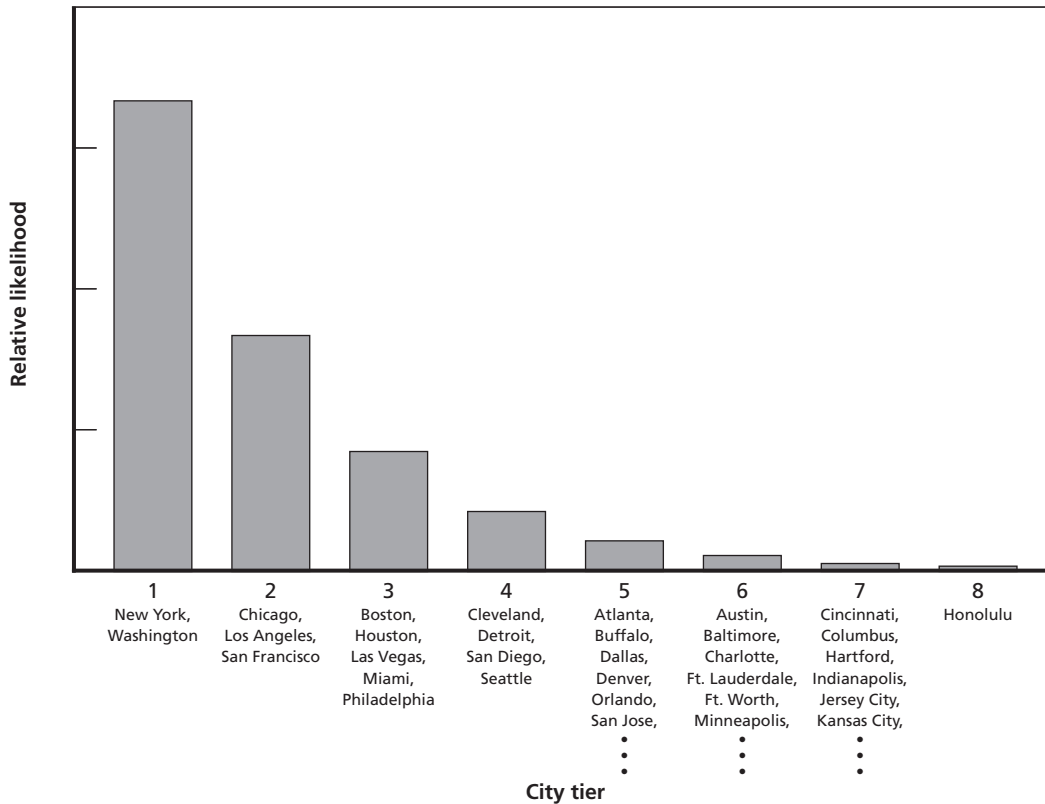
Values for both the relative likelihoods and absolute attack likelihoods are derived through a structured expert elicitation process that is informed by terrorist attack histories and contextual trends, such as mentions of particular cities and targets in Arabic media. Members of the expert advisory network consulted by RMS are listed in Appendix A. Expert elicitation conferences are held twice each year to update probability profiles with current information and analysis of terrorism. Details of how this process is carried out can be obtained from RMS.

For transparency into assumptions made when the RMS model is most typically used, results from the expert elicitation carried out in 2005 are discussed below. These figures are provided as a documentation of how RMS has assessed threat. Since threat is the most poorly understood element of terrorism risk, it is important to understand the specific assumptions that are made when estimating terrorism risk with the RMS model. It is also advisable to consider multiple perspectives about the likelihood of terrorist attacks whenever this or other models are used to estimate terrorism risk. If users disagree with any of the specific assessment, the assumptions could be changed, model estimates reobtained, and results compared to see how the assumptions affect estimates of terrorism risk.

### **Estimating City Tier Likelihood**

In its model, RMS groups cities into separate tiers according to relative likelihood of attack. RMS determines the city groups and attack mode likelihood for each tier in conjunction with its expert advisory network. Figure 2.2 shows that the model concentrates terrorist attack risk in the United States in a small number of cities. The 2005 threat assessment concluded that an attack is likeliest to occur in the five highest-ranked cities.

**Figure 2.2**  
**Relative Likelihood of Terrorist Attack in Different City Tiers**



RAND TR386-2.2

### Estimating Target Type and Individual Target Likelihoods

As with cities, RMS combines target types into separate groups according to the relative likelihood of attack. The target type groups and the likelihood of attack for each group are determined in conjunction with the RMS expert advisory network. The model includes 34 different target types that are divided into eight groups representing distinct levels of threat. Table 2.1 lists the target types included in each group as well as the 2005 expert judgment about the relative likelihood of attack for each group and the relative abundance of targets in that group included in the RMS target database. The RMS model also provides the ability to incorporate attack likelihoods for specific individual targets based on their iconic value and security status. The iconic value parameter allows the attack likelihood for individual high-profile targets, such as iconic buildings, to be increased. Conversely, the security parameter allows the attack likelihood for individual targets with particularly high security, such as the White House, to be decreased. In general, however, this feature is largely unused in the RMS model, because the specific information needed to assess these parameters for individual buildings is not available; that is, nearly all targets of a given target type are assigned the same iconic value and security



**Table 2.1**  
**RMS Target Type Groups**

Target Type Group	Target Types in Group
1	Government buildings
2	Business districts, skyscrapers, stock exchanges, hotels and casinos, airports, nuclear power plants
3	Military, train and subway stations, stadiums, bridges and tunnels
4	Industrial facilities, oil and gas processing facilities, tourist attractions, shopping malls, restaurants, ports and ships
5	Media HQ, Fortune 100 HQ, theaters, major entertainment centers, gas stations
6	Cruise ships, apartment buildings, foreign consulates, United Nations
7	Water reservoirs and distribution, passenger trains, airspace zones
8	Power plants, dams, railway networks

levels. Collecting and incorporating such data for specific localities or industry sectors would enhance the utility of the model.

Target type likelihoods in the RMS model are estimated independently of the city under consideration. For example, the model assigns the same relative likelihood of attack to a hotel in Las Vegas as it does to a hotel in any other city (city tier notwithstanding). While reason might suggest that hotels are at greater risk in Las Vegas, financial institutions are at greater risk in New York, and government buildings are at greater risk in Washington, D.C., there has not been an attempt to adjust the current model to reflect those additional factors. Adjusting the iconic value of specific targets could capture these dynamics.

### Estimating Attack Mode Likelihood

The RMS model accounts for the possibility of 37 types of terrorist attack. These attack modes, listed in Table 2.2, include attacks involving conventional weapons, weapons of mass effects, and sabotage of industrial facilities. Because the RMS model provides an assessment only of a macroterrorism event, it does not include events such as suicide bombings or sniper attacks, which would have smaller direct impacts. The expert elicitation process of attack mode likelihoods is informed, in part, by the notion of each attack mode's "logistics burden." The logistics burden is a cost assigned to each mode that reflects skill, labor, time, and financial resource requirements. More resource-intensive modes have higher logistics burdens, which tends to decrease their relative likelihood.

The relative likelihood of a terrorist attack depends strongly on the type of attack being considered. Figure 2.3 shows that the 2005 expert elicitation of the relative likelihood of an attack with a 600-lb bomb is much higher than that of the next highest likelihood attack mode, a 1-ton bomb. A 600-lb bomb is the smallest bomb size considered in the RMS model and is modeled as a passenger car-sized bomb. The relative likelihood of CBRN attacks is very low. Though the consequences of CBRN events are much larger, lower attack likelihood means that the risk from these events may be more comparable to that from conventional attacks.

**Table 2.2**  
**Modes of Attack Modeled in the RMS Terrorism Risk Model**

Attack Mode	Description of Attack Scenarios in Model
Surface-to-air missile	Commercial 747 airliner shot down
Bomb	600 lb; 1 ton; 2 ton; 5 ton; and 10 ton
Aircraft impact	Hijacked 747 commercial airliner flown into a target
Conflagration	9,000-gallon gasoline tanker hijacked and set on fire
Sabotage: industrial, explosion	5-, 50-, and 150-ton TNT equivalent
Sabotage: industrial, toxic release	5%, 40%, and 100% of Bhopal accident
Sabotage: industrial, explosion + release	5 ton + 5% Bhopal; 50 ton + 40% Bhopal; and 150 ton + 100% Bhopal
Sabotage: nuclear plant, radiation release	0.5%; 5%; and 20% of inventory
Dirty bomb: cesium 137	1,500 Curies and 15,000 Curies
Chemical: sarin gas	Indoors: 10 kg; outdoors: 10 kg, 300 kg, and 1,000 kg
2% anthrax slurry released outdoors	1 kg, 10 kg, and 75 kg of slurry
Weaponized anthrax released indoors	40 g of weaponized anthrax
Smallpox	10, 100, and 1,000 initially infected
Genetically engineered smallpox	100 and 1,000 initially infected
Nuclear bomb	1 kt and 5 kt

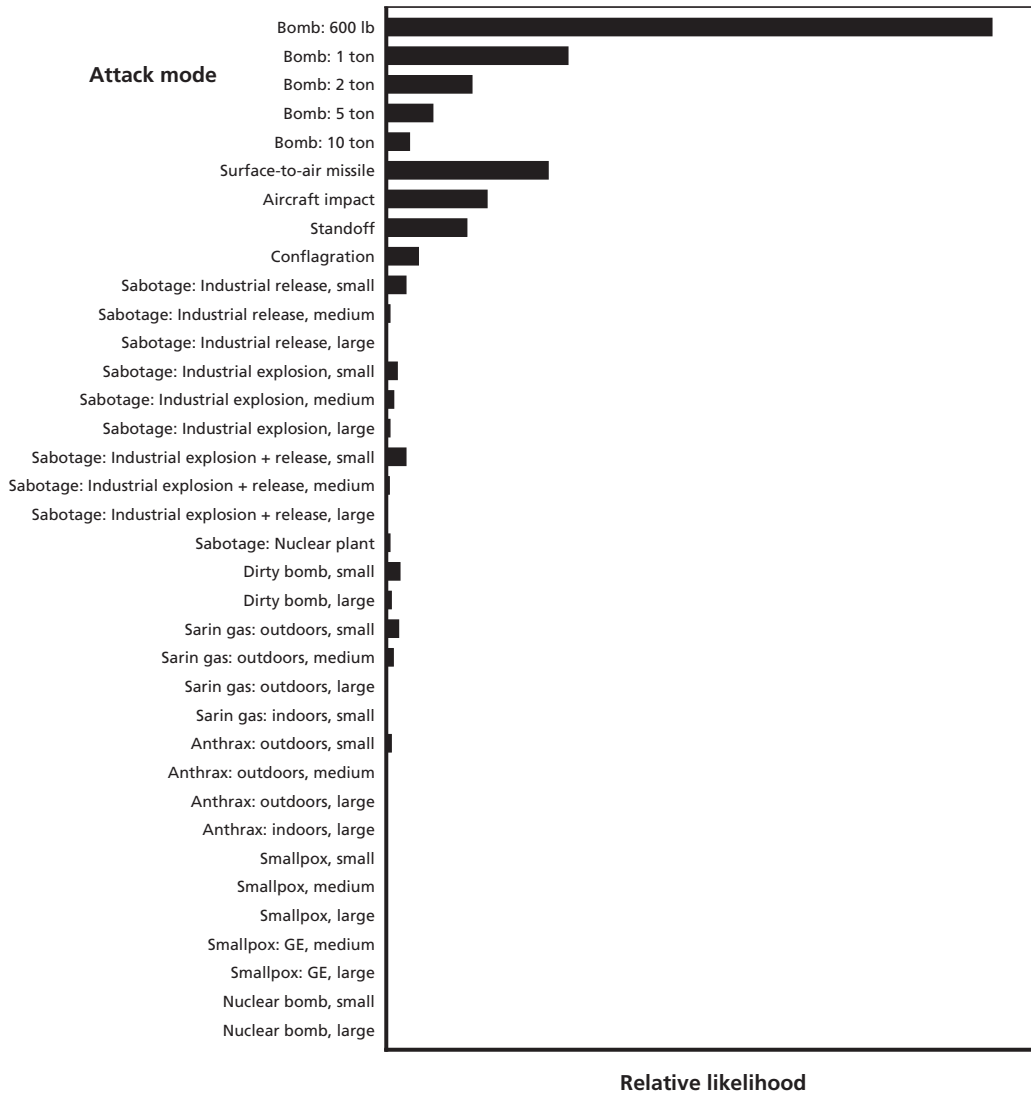
### Estimating Relative Attack Likelihood

The relative likelihood of attack in the RMS model accounts for the individual component likelihoods based on city tier, target type tier, individual target likelihood, and attack mode likelihood. Under the condition that an attack occurs, the relative attack likelihood determines where and what kind of attack will occur. The probability of any attack occurring is dictated by the absolute attack probability, which is discussed below.

One useful way to examine relative attack probabilities is to calculate the relative attack probabilities in different cities. The relative probability of any attack for a given city is the sum of the relative attack probabilities for all threat events evaluated in each city. The overall relative probability incorporates both the expert judgment of relative probabilities and the number and types of targets modeled for each city.

The number of events evaluated per city ranges from one for isolated terrorist targets to more than 2,000 in New York City. The relative probability of any attack in a given city provides a measure of the relative likelihood of a city being attacked that accounts for differences in the number of attacks evaluated in each city. Figure 2.4 shows this overall relative probability, expressed as the sum of the relative probabilities of all target–attack mode pairs (scenarios) modeled in each city as a function of the number of scenarios modeled for that city.

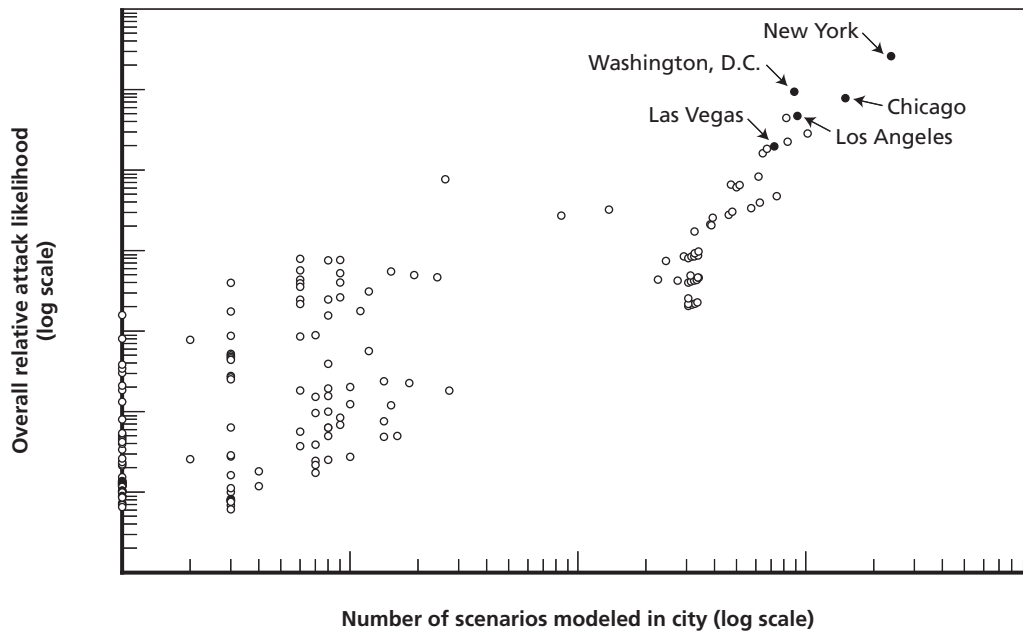
**Figure 2.3**  
**Relative Likelihood of Terrorist Attack for Different Attack Modes**



RAND TR386-2.3

The results show that the overall relative likelihood of attack is concentrated in a few cities. Four cities—New York, Washington, D.C., Chicago, and Los Angeles—account for most of the total attack likelihood in the country. Much of the concentration of terrorism likelihood in cities as calculated by the model results from the numbers of potential targets that have been identified there—cities with more locations believed to be attractive targets are, unsurprisingly, estimated to be at higher likelihood of attack, since there are many more options for terrorist attacks in these cities. However, classification of different types of target means that aggregate likelihood estimates are also shaped by our current understanding of which targets are more attractive to terrorists. For example, Washington, D.C., is a tier 1 city and has a

**Figure 2.4**  
**Overall Relative Attack Likelihood for Different Cities**



RAND TR386-2.4

disproportionate number of government buildings (tier 1 target types). This leads to its overall relative likelihood of attack being higher than would be expected if the distribution of target types in Washington, D.C., were more like the distribution of target types in the nation as a whole.

### Estimating Overall Attack Likelihood

To estimate the overall likelihood of attack, the RMS model incorporates expert judgments of the likelihood of any attack in the next year. Since it is possible that more than one event could occur in a given year, RMS uses a statistical simulation to assess the average probability that more than one event happens in any year. The statistical simulation allows for expert judgment on whether responses after an initial attack will change the probability that additional events are successfully attempted within the same year.

### Modeling Attack Consequences

Consequences of terrorist attack scenarios in the RMS model are estimated from three components: weapon effects, target characteristics, and exposure characteristics. Weapon effects comprise the type of weapon, the delivery mechanism, the hazards to people and property, and the spatial and temporal footprint of those hazards. A 600-lb bomb, for example, is detonated in a car, and damage occurs from blast pressure waves and debris impact that extends for tens of meters around the blast site. For each attack mode listed in Table 2.2, RMS has developed

comprehensive physical event models that generate a hazard footprint that specifies a hazard level estimate as a function of location around the attack site. The size of the hazard footprint can vary from less than 100m (e.g., for a small bomb) to several hundred square kilometers (e.g., for a nuclear or outdoor biological attack).

Target characteristics include building features for each target that influence the attack consequences. These include height, number of stories, year built, and construction type. Characteristics may also include other factors specific to a particular target type. These target characteristics help define the vulnerability of people and structures to the hazard imposed by the weapon. For example, newer steel buildings will suffer less damage from a bomb than will older masonry buildings. Building characteristics are compiled from multiple sources, including the data from the Sanborn Map Company.<sup>3</sup>

The attack exposure refers to the population and structures impacted by an attack. The exposure includes the number and spatial distribution of people within the hazard footprint as well as (for insurance loss calculation purposes) their occupational status and age distribution. The exposure also accounts for the characteristics and density of structures within the hazard footprint. Exposure characteristics determine the losses from an attack in terms of the casualty distribution and property damage. Estimates of the number and demographics of building occupants are derived from local census data, journey-to-work data, building-use type, and building size. The number of occupants is also adjusted to account for the time of day. This study examined the effects of midafternoon, weekday attacks. Most buildings, except for residential ones, would be most fully occupied at this time; therefore, the estimates reflect the worst case in the sense of the number of people exposed to the attack.

The model estimates damage from an attack in terms of casualties and property losses. The model provides estimates of the number of victims in each of six different casualty categories: medical only; temporary, total disability; permanent, partial, minor disability; permanent, partial, major disability; permanent, total disability; and fatality.<sup>4</sup>

Property damage in the RMS model includes dollar losses to buildings and building contents as well as business interruption losses. Building and building content losses represent the replacement value of damage to property. Business interruption losses represent losses resulting from a civil authority exclusion zone around the incident site; this includes losses only from business closure in this area and does not include indirect losses from business interruptions in other areas that are caused by these closures or changes in consumer activity as a reaction to terrorist events.

## **Applicability of the RMS Model to DHS Decisionmaking**

It is important to identify the scope and purpose of the RMS model and how these may impact its applicability to informing decisionmaking about homeland security efforts. Because it is

---

<sup>3</sup> The Sanborn Map Company maintains spatial coordinates as well as numerous building attributes for buildings in major metropolitan areas across the United States.

<sup>4</sup> These categories correspond to standard definitions used for workers' compensation lines of business.

designed to help the insurance industry estimate and manage risk, the RMS model focuses on estimating risk in terms of insured loss. This has two important implications for what is and is not included in the model. The target database includes more than 3,000 urban facilities and buildings. As noted previously, targets were selected based on the criteria that an attack could produce economic losses in excess of \$1 billion, more than 100 fatalities or 500 injuries, or massively symbolic damage. While this target database is expected to overlap in large measure with targets of interest identified by DHS through other means, some important targets may be missing. This stems from the fact that the objective of the RMS model is to characterize risk in terms of insured losses; it does not consider interdependencies among critical infrastructures or economic systems that could result in broader indirect or macroeconomic consequences of terrorist attacks. Consequently, targets with low insured value but that may still result in large indirect losses and major disruption in the event of an attack, such as communication and energy infrastructure, are underrepresented compared to other target lists (e.g., DHS, 2003). Nevertheless, adding targets to the model is feasible and could enhance its value to DHS.

There are also other potential gaps in the current RMS exposure database that stem from its development for the insurance industry. For example, the model does not account for the value of government buildings or the number of government employees, because governments generally self-insure. In addition, the model generally 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. For the same reason, the model does not include stadium spectators or passengers in airport terminals and planes. Assuming that the relevant occupancy, spectator, and passenger data are available, addressing many of these issues is straightforward.

## Application 1: Terrorism Risk in UASI Areas

---

DHS is responsible for leading the nation's unified effort to prevent and deter terrorist attacks and protect against and respond to threats and hazards to the United States. UASI is intended to help meet these responsibilities by providing resources to select urban areas for planning, equipment, training, exercises, and program management and administration. In 2005, the UASI program allocated \$830 million to 50 urban areas. According to the homeland security grant program guidance kit, UASI funding allocations were based on a formula that accounted for credible threat, presence of critical infrastructure, vulnerability, population, population density, law enforcement investigative and enforcement activity, and the existence of formal mutual aid agreements (DHS, undated).

In 2006, HITRAC was tasked to support the grant allocation process by assessing terrorism risk for the UASI-eligible urban areas. This directive was the motivation for the first application in this study, which addressed three questions:

1. How is terrorism risk distributed across UASI cities?
2. Is the distribution of RMS's terrorism risk estimates different when measured as property risk versus fatality risk?
3. How does the distribution of RMS risk estimates differ by attack mode?

This case study provided evidence that the RMS model can support resource allocation decisionmaking. Terrorism risk estimates were found to be highly concentrated in relatively few of the UASI-eligible urban areas. Furthermore, with a few exceptions (Las Vegas, Miami, and Santa Ana/Anaheim), the distribution of risk estimates is not sensitive to whether risk is measured as property damage or fatalities. However, the distribution can vary dramatically based on which attack modes are considered.

This case study also highlighted several paths to making the RMS model more useful for resource allocation decisionmaking:

- The model databases, particularly the target database, should be compared to other data sets and possibly expanded.
- The consequence model should be linked to other models of indirect economic effects to understand the relative importance of the consequences of interconnected or interdependent infrastructure systems.

- These results should be compared to analyses using different assumptions about terrorist threats as well as different models, including those that address natural disaster risk.
- 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 to terrorism risk.

## Methodology

Terrorism risk estimates were calculated for each of the UASI-defined urban areas for fiscal year 2005. This analysis assessed terrorism risk in 45 urban areas. Appendix C lists these areas and how they are geographically defined. These 45 areas encompass all 50 urban areas that received separate funding allocations. However, several urban areas were analyzed as larger metropolitan areas, either because the information provided or the design of the RMS model did not allow for separate analysis. Specifically, the areas of Anaheim and Santa Ana, California; Los Angeles and Long Beach, California; Jersey City and Newark, New Jersey; and Arlington, Dallas, and Fort Worth, Texas, were analyzed as combined areas.

Risk estimates were calculated using estimates of the average annual fatalities and average annual loss (AAL) of property as measures of consequences. Property loss risk included the total value of damage to buildings and contents but did not include RMS estimates of business interruption losses. Average annual consequences are the probability-weighted sum of the calculated losses for events modeled in the Probabilistic Terrorism Model. In this analysis, losses are summed across all events modeled and are aggregated by urban area. Results in this chapter are presented either as expected consequences or as shares of total risk estimates for all urban areas modeled.

These risk estimates rely on the assumptions about terrorism threat that were captured through the expert elicitation process that RMS conducted in 2005. Appendix A lists the terrorism experts consulted by RMS through this process. Chapter Two provides specific details about the threat assumptions made in this assessment.

Results are presented as risk shares, where the risk share is defined as the risk for a specific urban area divided by the sum of risk across all urban areas. For example, consider two urban areas that have expected annual fatalities from terrorism of one and three. In this case, the corresponding risk shares would be 0.25 and 0.75, respectively. Note that, because risk shares represent a percentage of the total risk estimates, changes in one value affect all the other values.

Risk estimates were modeled using several sets of attack modes. The standard analysis was conducted with a set that included all attack modes considered in the RMS model (see Table 3.1). These attack modes have considerable overlap with the Homeland Security Council (HSC) national planning scenarios. Table 3.1 lists the HSC scenarios and how they compare to events covered in the RMS methodology. The corresponding RMS scenario was chosen to reflect an attack of relatively the same magnitude and via the same generic damage mechanisms. The RMS attack modes represent a larger number of scenarios. The RMS set provides for more sensitivity analysis of assumptions about some of these threats by providing alternatives that vary basic threat assumptions, such as the size of a bomb or chemical release. There are a few



**Table 3.1**  
**Homeland Security Council National Planning Scenarios and Comparable RMS Scenarios**

HSC Scenario	Corresponding RMS Scenario
Nuclear detonation: 10 kt	5 kt nuclear detonation
Biological attack: anthrax	Small, outdoor anthrax attack
Biological disease: flu pandemic	Not included in RMS terrorism model, but infectious disease is represented through smallpox
Biological attack: pneumonic plague	Not included in RMS terrorism model, but infectious disease is represented through smallpox
Chemical attack: blister agent	Small, outdoor sarin gas attack
Chemical attack: toxic industrial chemicals	Large industrial sabotage with explosion and chemical release
Chemical attack: nerve agent	Small, indoor sarin gas attack
Chemical attack: chlorine tank explosion	Small industrial sabotage, release only
Natural disaster: major earthquake	Not included in RMS terrorism model
Natural disaster: major hurricane	Not included in RMS terrorism model
Radiological attack: dirty bombs	Small dirty bomb
Explosives attack: improvised bombs	600-lb trinitrotoluene (TNT) car bomb
Biological attack: food contamination	Not included in RMS terrorism model
Biological attack: foot-and-mouth disease	Not included in RMS terrorism model
Cyber attack	Not included in RMS terrorism model

NOTE: For further details on each of these scenarios for this table, see RMS (2005).

important exclusions in the RMS model. Specifically, flu, earthquakes, hurricanes, food-borne illness, foot-and-mouth disease, and cyberattacks are part of the HSC scenarios but are not included in the RMS model. Flu is not included, at least in part because infectious disease is already considered through smallpox incidents. Earthquakes and hurricanes are not part of RMS terrorism models but are included in RMS's other catastrophe models. Food-borne illness and foot-and-mouth disease are simply not modeled at this time by RMS. Finally, cyberattacks are not modeled because the consequences are largely the result of interconnected systems, which are not reflected in the RMS model.

Next, three separate analyses were conducted for subsets of the full attack mode list in Table 3.1. First, an analysis was conducted considering only attack modes associated with improvised bombs, aircraft impact into buildings, and conflagration (i.e., explosion of a gasoline truck). This grouping reflected attack modes that required modest capability and resources to accomplish and for which risk was related to the number of target assets a city has. The second analysis included only CBRN weapon attack modes. This aggregation reflected attack modes for which consequences affect a large area and for which each city becomes a potential target. In addition, available countermeasures for CBRN attacks are likely very different from those for conventional attacks. Finally, the third grouping, referred to as sabotage, included

only those attack modes directed at industrial facilities. In the RMS model, sabotage is modeled at oil refineries, chemical plants, and nuclear power plants that are in the model's target database. A distinguishing characteristic of these attack modes is that they are associated with very specific infrastructure target assets.

## Results of Analysis

RMS calculations provide estimates of the distribution of terrorism risk among UASI-eligible urban areas. Analyzing this distribution leads to several observations that could be used to inform resource allocation decisionmaking.

### How Is Terrorism Risk Distributed Across UASI Cities?

Figure 3.1 presents RMS estimates for the fraction of terrorism risk for each UASI-eligible area based solely on estimates of expected fatalities. RMS estimates (black diamonds) for the share of average annual fatalities are compared to the proportion of the total UASI-covered population for each city (open circles), the share of UASI funding (open triangles), and equal allocation (black line). This figure highlights two observations. First, terrorism risk is highly concentrated in a small number of UASI-eligible areas. According to these RMS estimates, two cities in particular carry a disproportionate share of the terrorism risk burden: Chicago and New York. More than 95 percent of the risk is concentrated in only eight of the cities (New York, Chicago, Washington and the capitol region, San Francisco, Los Angeles, Boston, Houston, and Philadelphia). A third group of 18 cities (Jersey City and Newark through Buffalo) have little risk.<sup>1</sup> Together, these cities account for about 4.5 percent of the remaining terrorism risk. According to these RMS estimates, the remaining 19 urban areas have negligible terrorism risk. Together, they account for only 0.1 percent of the RMS risk estimates.

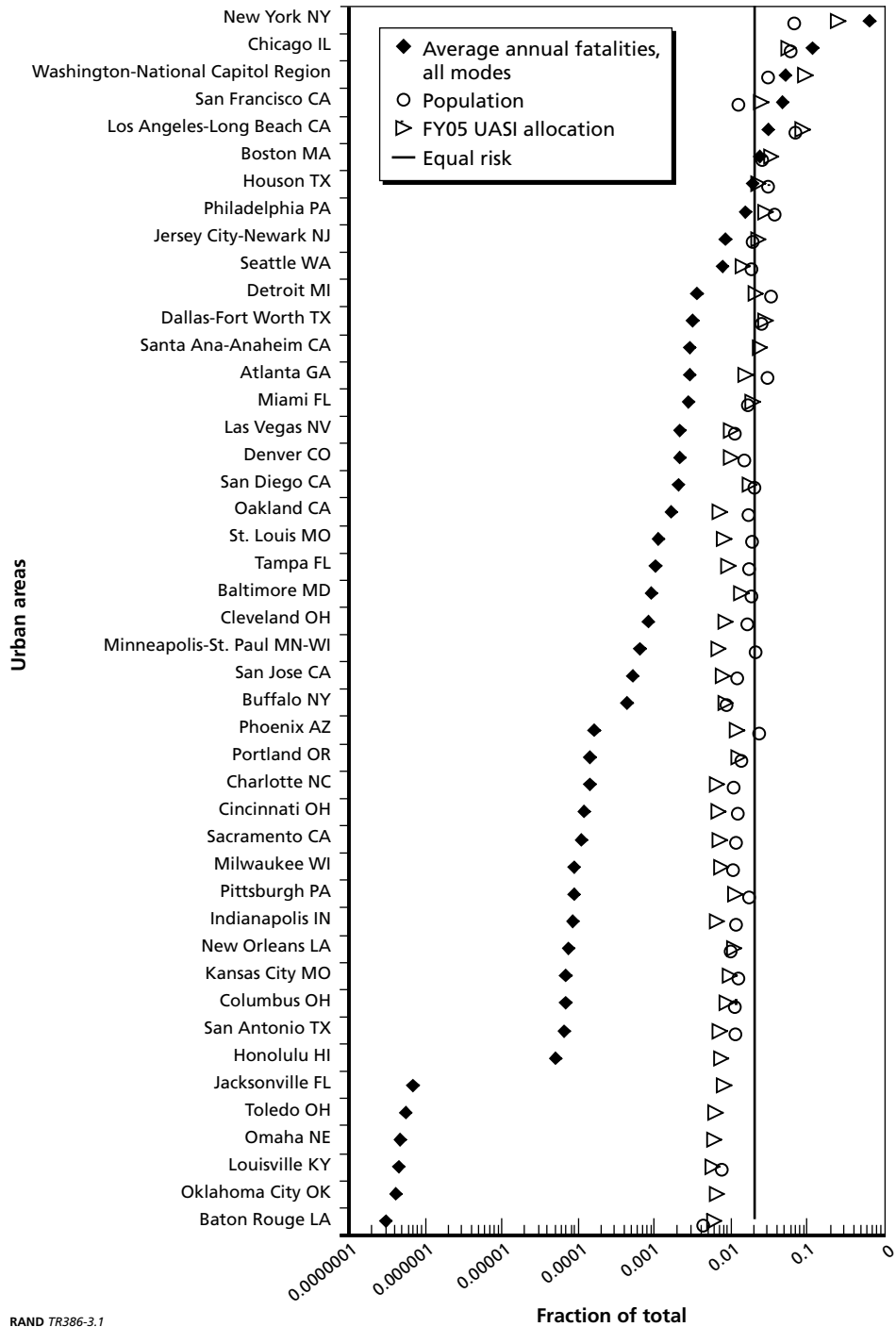
Second, the estimated proportion of terrorism risk in each urban area exceeded the share of population and the actual UASI allocation percentages in only three urban areas: New York, Chicago, and San Francisco. Interestingly, Washington and the capitol region appear to have a disproportionate share of terrorism risk compared to the region's population, but the share of UASI allocations exceeded the share of estimated terrorism risk. For all other urban areas, estimated terrorism risk shares fall below both the distribution of population and UASI allocations.

The differences between relative amounts of UASI funding and our risk estimates using the RMS model are substantial and warrant further examination. They raise important questions about the content of the RMS model and its assumptions—in particular, which targets are included in the RMS target database and how important the indirect effects of terrorism might be that are not included. Both these issues are discussed in further detail later in this chapter.

---

<sup>1</sup> Las Vegas, which was analyzed individually in Chapter Four, is in this group of urban areas. Though Las Vegas is estimated to have the ninth highest overall attack likelihood, Las Vegas's position is lower (sixteenth) in terms of estimated fatality risk shares. This is because risk estimates reflect both likelihood and consequence and therefore account for the density and amount of surrounding population and property value—factors for which Las Vegas is exceeded by larger, higher-density urban areas.

**Figure 3.1**  
**RMS Probabilistic Terrorism Model Estimates for the Fraction of Total Risk for**  
**Each of the Urban Areas Eligible for UASI Funding in 2005, Considering All Attack**  
**Modes**



At the same time, these differences may indicate that the current UASI funding scheme allocates too much funding to lower-risk areas and too little funding to higher-risk areas.

### **Is the Distribution of RMS Terrorism Risk Estimates Different When Measured as Property Risk Versus Fatality Risk?**

While the previous discussion focused entirely on risk measured in fatalities, some citizens and decisionmakers are also concerned about the property losses from terrorism. Therefore, we also estimated terrorism risk in terms of the direct economic consequences from the loss of property, both building structures and their contents. Figure 3.2 compares the share of RMS risk estimates as measured in terms of average annual fatalities and AAL of property.

Overall, the distribution of terrorism risk by property damage is very similar to the distribution by fatalities. Once again, New York and Chicago carry a disproportionate burden of risk; more than 95 percent of risk is concentrated in only nine cities (adding Jersey City and Newark); and the remaining cities have little to no risk. The average absolute difference between the property value and fatality risk shares is only 0.3 percent. The largest differences occur in the cities with the largest risk and range in magnitude from 1 percent to 3 percent.

The comparisons in Figure 3.2 highlight cities that have disproportionately high property values for their population or vice versa. For example, Las Vegas appears to have a higher share of property value risk than fatality risk. This corresponds to the fact that the casinos in Las Vegas have high property values and that Las Vegas is a medium-sized (albeit rapidly growing) city.<sup>2</sup> In contrast, the region of Santa Ana and Anaheim have a lower share of property value risk than fatality risk. This is presumably a result of the relatively large population in the region and the absence of a large, high-value, central business district. Note that the use of a logarithmic scale in Figure 3.2 exaggerates the apparent differences for cities like Las Vegas, Miami, and Santa Ana/Anaheim as compared to those for cities with larger risks.

### **How Does the Distribution of RMS Risk Estimates Differ by Attack Mode?**

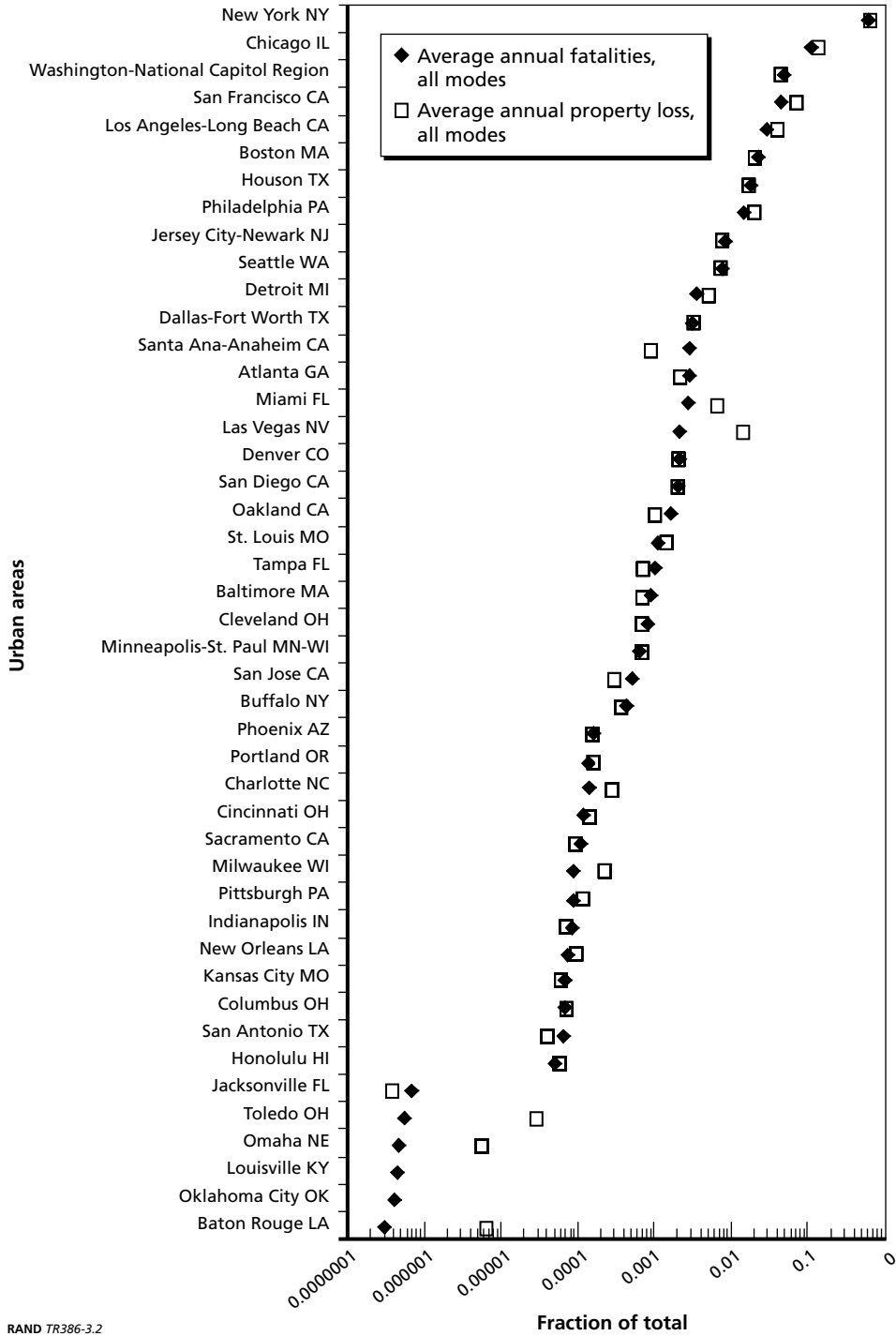
Risk can also differ by attack mode. The observation that risk estimates are concentrated in a few cities is consistent across conventional and CBRN attack modes. However, there are unique differences in the distribution that affect certain cities. This becomes important when considering new intelligence about the potential capabilities and intent of terrorist groups or how resources might be spent on countermeasures that may be effective against one class of attack modes.

The comparisons in Figures 3.3, 3.4, and 3.5 provide insight into how terrorism risk appears to differ among conventional, CBRN, and industrial sabotage attack modes. Figure 3.3 compares terrorism risk by all modes to terrorism risk by only conventional modes. Recall that these figures present shares of risk, not absolute risk, so the changes in one (e.g., New York City) value affect all the other values. From this figure, it is clear that terrorism risk in most cities is lower when only conventional attack modes are considered. In fact, terrorism risk estimates

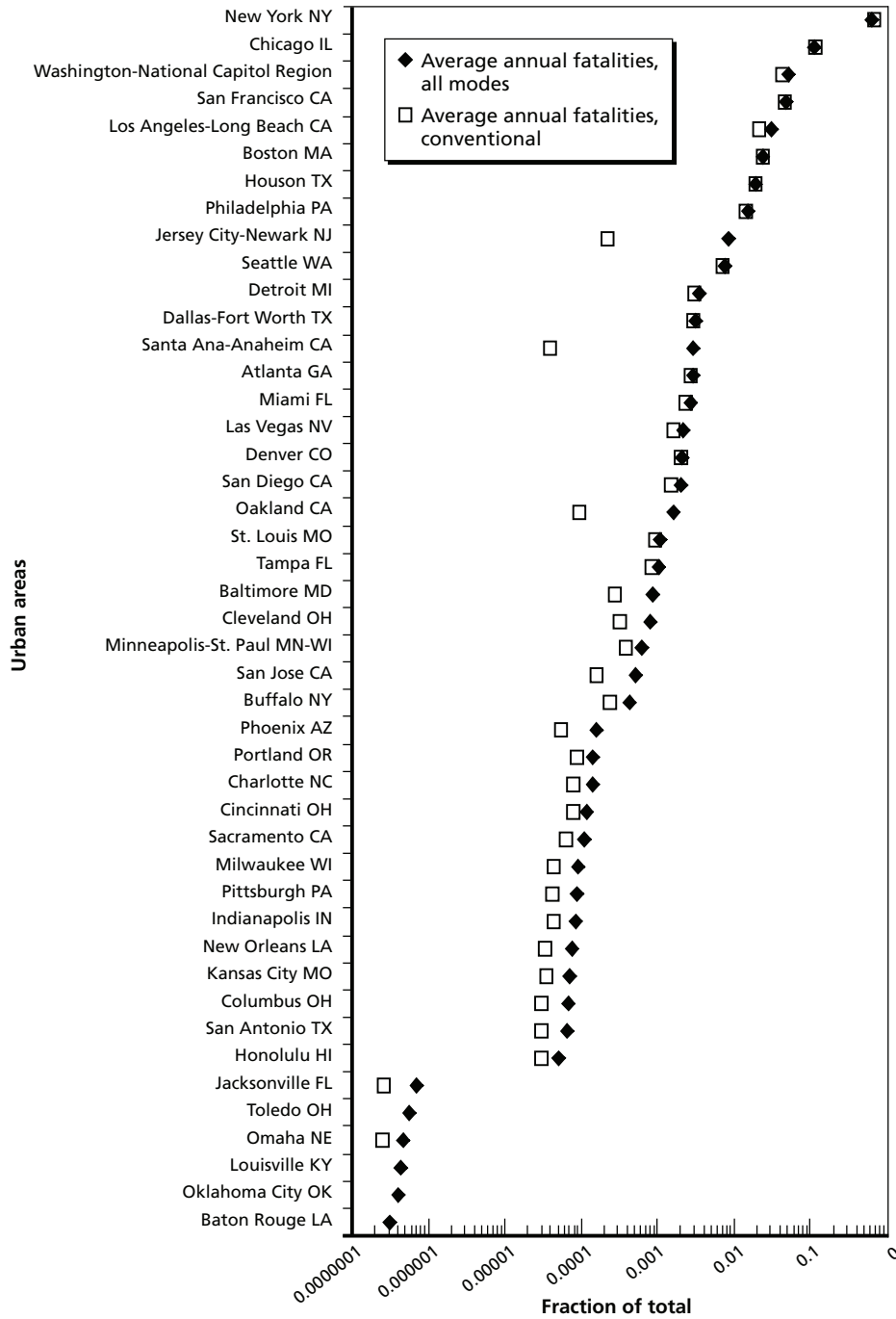
---

<sup>2</sup> Also note that, as discussed in Chapter Four, the RMS model does not include fatalities of hotel guests. While correcting for this assumption would change the expected fatalities of Las Vegas, it is expected that it would also change the expected fatalities of other large cities with many hotels, like New York, Washington, and Chicago.

**Figure 3.2**  
**Comparison of RMS Probabilistic Terrorism Model Estimates for the Fraction of Total Risk for Each of the Urban Areas Eligible for UASI Funding in 2005 in Fatalities Versus in Property Losses, Considering All Attack Modes**

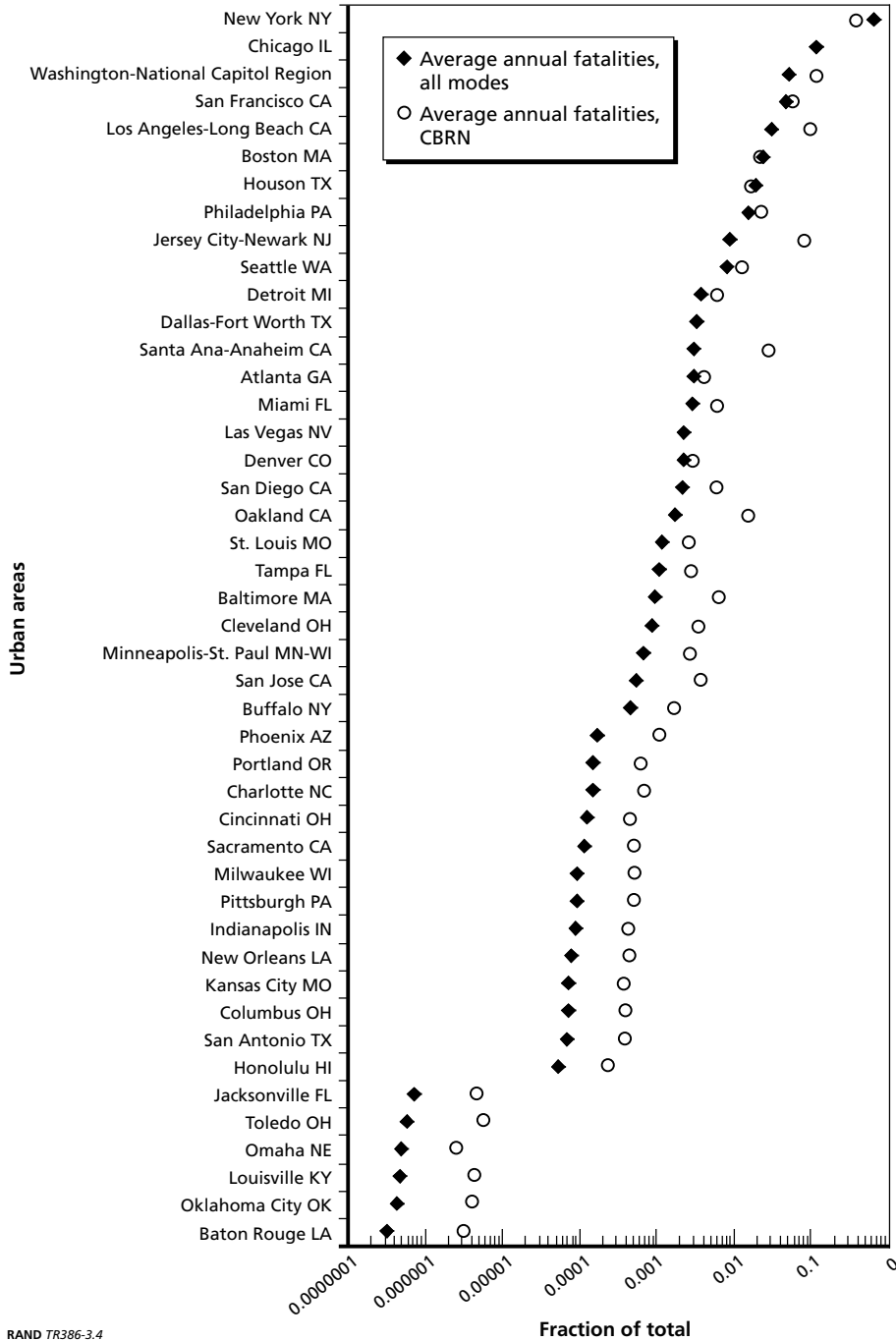


**Figure 3.3**  
**Comparison of RMS Probabilistic Terrorism Model Estimates for the Fraction of Total Risk for Each of the Urban Areas Eligible for UASI Funding in 2005, Considering All Attack Modes Versus Conventional Attack Modes Only**



NOTE: For each city, the combination of percentages for conventional, sabotage, and CBRN equals 1.0.

**Figure 3.4**  
**Comparison of RMS Probabilistic Terrorism Model Estimates for the Fraction of Total Risk for Each of the Urban Areas Eligible for UASI Funding in 2005, Considering All Attack Modes Versus Chemical, Biological, Radiological, or Nuclear Attack Modes Only**







by conventional attack modes are higher than risk estimates for all attack modes only in New York and Chicago, where the differences between the estimates are 4 percent and 0.3 percent, respectively. The net effect is that a relatively large increase in New York City's risk estimate produces a small decrease in all other cities' shares of risk. The average decrease across the other cities is 0.09 percent. The comparison between estimates from all attack modes and only CBRN attack modes yields the opposite observation. As Figure 3.4 shows, risk estimates for CBRN attacks are lower than when considering all attacks in New York and Chicago, with differences of 27 percent and 2 percent, respectively. In contrast, risk estimates are higher in all other cities, with the largest differences being for the regions of Washington and the National Capitol Region (6.5 percent), Los Angeles and Long Beach (6.3 percent), and Jersey City and Newark (7 percent). These differences reflect the fact that risk affects the area and (in the case of Jersey City and Newark) its near neighbors (i.e., New York City) and that it is a function of each city being a target. These characteristics are in contrast to conventional attack modes, in which risk is a function of more localized consequences and the number of target assets within a city.

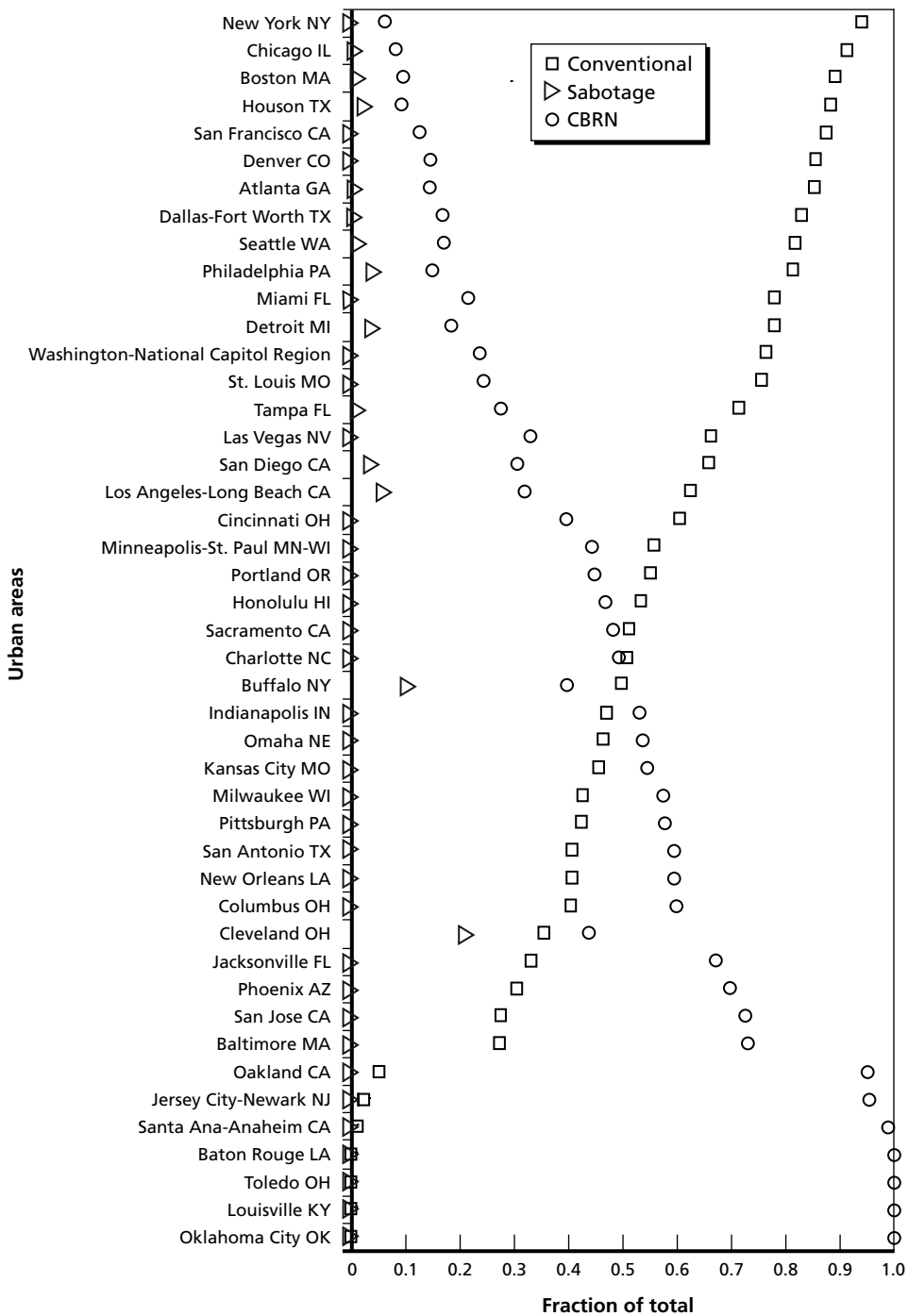
Finally, the distribution of risk for sabotage attack modes is very different from others presented previously. Figure 3.5 shows that the shares of sabotage risk estimates are concentrated in fewer and different cities than shares of risk considering all attack modes. For example, New York City carries only 2 percent of the estimated sabotage risk. Los Angeles and Long Beach, on the other hand, carry the greatest burden of estimated sabotage risk (36 percent). Perhaps the most important observation from this figure, however, is that, according to the model, 18 urban areas have no sabotage risk. This highlights the fact that sabotage risk is dependent on the presence, concentration, and collocation of specific types of industrial facilities with centers of population and property value.

The RMS terrorism risk model for the sabotage attack mode includes only chemical plants, oil refineries, and nuclear power plants. This, of course, raises the question of how complete the RMS target database is for the types of facilities included and the breadth of the types of facilities covered. In principle, the RMS model could be modified to include other facilities or types of facilities as targets.

Figure 3.6 provides further data to support the observations discussed previously. In this figure the  $y$  axis represents the fraction of a city's risk that is accounted for by each category of attack mode. Thus, for each city, the fractions of conventional, CBRN, and sabotage risk sum to 1.

Three observations are evident in Figure 3.6 and help explain those discussed previously. First, large cities that have a high density of both population and property value and also have a large number of target assets (e.g., skyscrapers, large corporation headquarters, government buildings) tend to have a large percentage of estimated risk being associated with conventional attack modes. Conventional terrorism represents the dominant component of risk in some cities (e.g., New York City, 94 percent; Chicago, 91 percent; Boston, 89 percent). This does not mean that the magnitude of other sources of risk in these cities is low. New York City, after all, does have the highest estimated share of CBRN risk at 38 percent (see Figure 3.4). Rather, despite the consequences of CBRN attack, the judged low probability of such occurrences when compared to the combined higher probability and large number of target

**Figure 3.6**  
**Percentage of Terrorism Risk for Each of the Urban Areas Eligible for UASI Funding in 2005 by Category of Attack Mode**



NOTE: For each city, the combination of percentages for conventional, sabotage, and CBRN equals 1.0.

assets for conventional attacks leads to the estimated terrorism risk in New York City being largely from conventional attack modes.

Second, and parallel to the first observation, risk estimates for smaller cities with fewer target assets are dominated by CBRN risk. For example, the terrorism risk estimates for Baton Rouge, Toledo, Louisville, and Oklahoma City are entirely from CBRN events. Since every city is potentially a target for CBRN attacks, risk estimates for cities with few target assets will be dominated by CBRN risk. The observation that Oklahoma City, in particular, is dominated by CBRN risk again draws attention to important model assumptions, since, prior to September 11, 2001, it was the site of the largest terrorist attack on U.S. soil. As already discussed, one must consider and review the target database for both breadth and depth. Further consideration should also be given to the expert judgments about the relative and absolute probabilities of attacks of different types on different targets. As discussed again subsequently, the RMS model captures the results of a single expert-elicitation process, and different experts might produce different risk estimates. Comparing across both risk estimates and models could help to inform decisionmaking.

Finally, once again, sabotage risk constitutes a substantial portion of terrorism risk in only select cities. As discussed above, this is driven primarily by the dependence of sabotage scenarios on specific types of target and the distribution of these targets in the RMS target database.

## Conclusions About Risk and Observations About the Model

The results presented previously provide a description of terrorism risk that could be useful for informing resource allocation. However, this description must be used only with a strong understanding of the assumptions underlying the RMS model design and implementation.

RMS terrorism risk estimates suggest that risk from terrorism is concentrated in relatively few cities. Thus if these risk estimates are accurate (or even nearly so), expenditures on all 50 cities may not be warranted. While most observations discussed previously consider only expected annual fatalities, they are largely consistent with those made when considering potential property losses. Thus a shift in perspective of fatalities versus population might change allocations little but would perhaps change the attractiveness of countermeasures that are used. Finally, sabotage risk is unique to urban areas with specific types of infrastructure assets collocated with centers of high population and property value. One approach to allocation, rather than expanding an overall preparedness grant program to include them, would be to consider focusing directed investment specifically on these types of assets. DHS's Buffer-Zone Protection Program includes some aspects of this type of approach. All the important caveats to these conclusions about terrorism risk in UASI-eligible urban areas have already been made in this or previous sections. Risk estimates are dependent on the breadth and depth of the target database. Tremendous uncertainty surrounds estimates of terrorism threat, and thus analysis using different expert elicitation would improve this risk modeling. The exposure database has been designed to inform the insurance industry. Thus in cases in which excluded populations are important (e.g., government employees in Washington, D.C., or hotel guests in Las

Vegas), care must be taken to understand the implications of the underlying assumptions in the exposure database. Finally, the RMS model accounts only for direct effects of terrorism. It does not account for indirect effects associated with interconnected infrastructures or with risk from natural disasters. As a result, not only are the interdependencies of attacks in these cities not included, but also attacks on some infrastructure in remote locations that could have major effects on the country are not considered in this analysis. Each of these may be captured by other modeling techniques, and it is likely more appropriate to develop approaches for linking results of these modeling approaches together than simply to extend or expand the RMS terrorism risk model calculations.

In principle, all of these issues can be addressed. Target and exposure databases can be audited and, if necessary, expanded with available data. Results from the RMS model can be compared to other terrorism risk models or to other analyses using the RMS model, but with different expert elicitations to inform judgment of terrorism threat. Risk estimates and analytic approaches presented here can be linked to models that address indirect impacts and natural disaster risk. Pursuing any or all of these approaches would be useful as DHS continues to mature the application of risk-based budgeting and resource allocation.

## Application 2: Profiling Terrorism Risk in Las Vegas

---

This chapter presents the results of analysis using the RMS Probabilistic Terrorism Model to assess terrorism risk in Las Vegas, Nevada. This study was intended to explore how the RMS model can be used to assess terrorism risk within a given urban area. Las Vegas was chosen to allow OI&A to draw comparisons to parallel work being conducted within OI&A using different models. Since terrorism risk analysis requires assessment of significant uncertainties surrounding estimating threat, vulnerabilities, and consequences, it is especially important to consider results of different models that may lead to either complementary or conflicting conclusions.

The RMS model can be specifically used to address three questions relevant to OI&A's mission:

1. How does the overall terrorism risk in Las Vegas compare to that in other cities?
2. How do potential terrorist attack targets in 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?

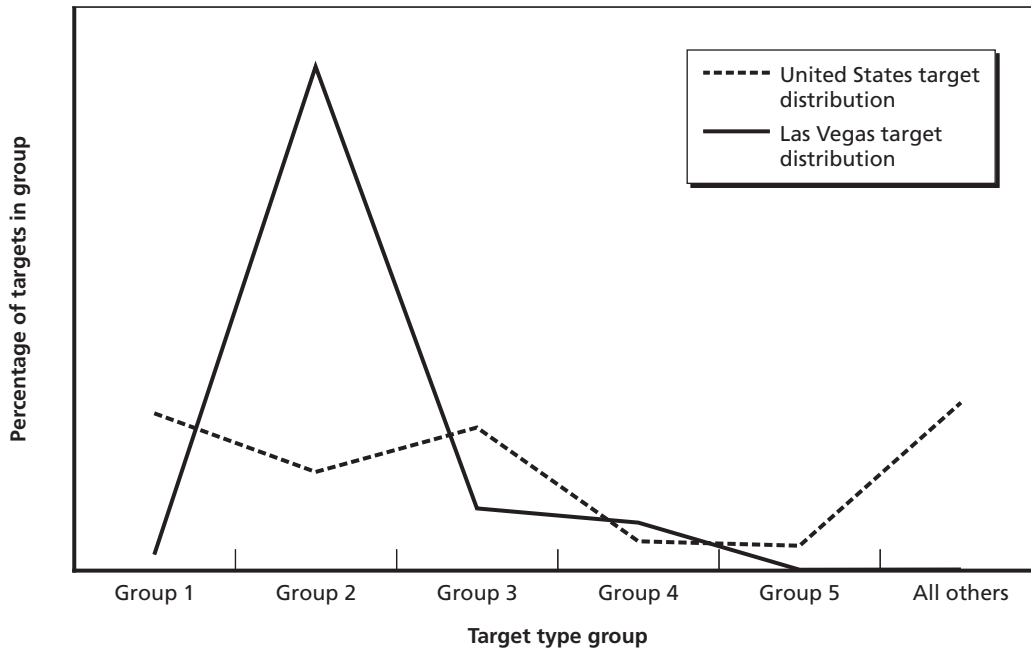
An important additional issue that this chapter addresses is the strengths and weaknesses of using models developed for the insurance industry to inform public sector homeland security decisionmaking.

### Attack Probabilities in Las Vegas

The threat assessment portion of the RMS model provides a structured way to explore how terrorism risk is distributed in an area, based on current views of terrorist intentions and capabilities. Figure 2.2 in Chapter Two shows that the RMS model classifies Las Vegas as a tier 3 city in terms of terrorism risk, placing it among the top 10 likeliest cities to be attacked.

In terms of targets included in the model, Las Vegas stands out in having a high proportion of high-likelihood targets compared to the nation as a whole. Figure 4.1 shows the distribution of targets within the RMS database according to target type for both Las Vegas and the entire country. A large majority of the targets in Las Vegas are classified as being in group 2, primarily being hotels, casinos, and skyscrapers (see Table 2.1 in Chapter Two). This unusual distribution increases the overall attack probability in Las Vegas relative to other cities in the same city likelihood tier.

**Figure 4.1**  
**Distribution of Targets by Group in Las Vegas and the Entire Country**



RAND TR386-4.1

Because of the high proportion of hotel-casinos in Las Vegas, and because a hotel-casino can be considered an iconic target type in Las Vegas, we conducted a sensitivity analysis (discussed below) to examine the effect of increasing the relative likelihood of hotel attacks in Las Vegas. The high city tier and the high proportion of tier 2 target types combine to generate a high overall attack likelihood in Las Vegas.<sup>1</sup> As shown in Figure 2.4 in Chapter Two, Las Vegas has the ninth highest overall attack likelihood or probability in the country.

## Consequences of Terrorist Attacks in Las Vegas

We begin by examining the consequences of a 600-lb bomb, the highest-probability attack type according to the model. There are many important outcomes that could be used to measure consequences. The most commonly mentioned measures for terrorism risk are fatalities and property damage (i.e., buildings and building contents). The RMS model calculates expected annual fatalities, injuries, property damage, and business interruption losses. In this chapter, we present results of expected annual fatalities and property damage to give examples of how measures of risk change with measures of consequence. For the sake of simplicity in presentation, we present one measure of consequence at a time.

<sup>1</sup> The overall attack likelihood is the sum of the relative likelihood of all attack mode–target pairs for a city.

Figure 4.2 shows the estimated number of fatalities for a 600-lb bomb attack at each of 68 modeled target locations in Las Vegas. Targets are grouped by target type. The variation in calculated expected fatalities is the result of differences in model assumptions about population densities around targets and vulnerabilities of different targets because of their size (height and area) and building materials.

The greatest potential fatalities for a 600-lb bomb in Las Vegas are in the large hotel-casinos. As noted previously, hotel-casinos, along with central business districts, are the most common target types in Las Vegas. The high values for the railway stations reflect the fact that most railway stations in Las Vegas are often collocated in hotels, so they are not actually separate targets. Similarly, targets may be in two categories, as is the case with some skyscrapers that are also hotels. For instances in which this occurs, aggregated risks consider targets to be only the class that results in greatest risk.

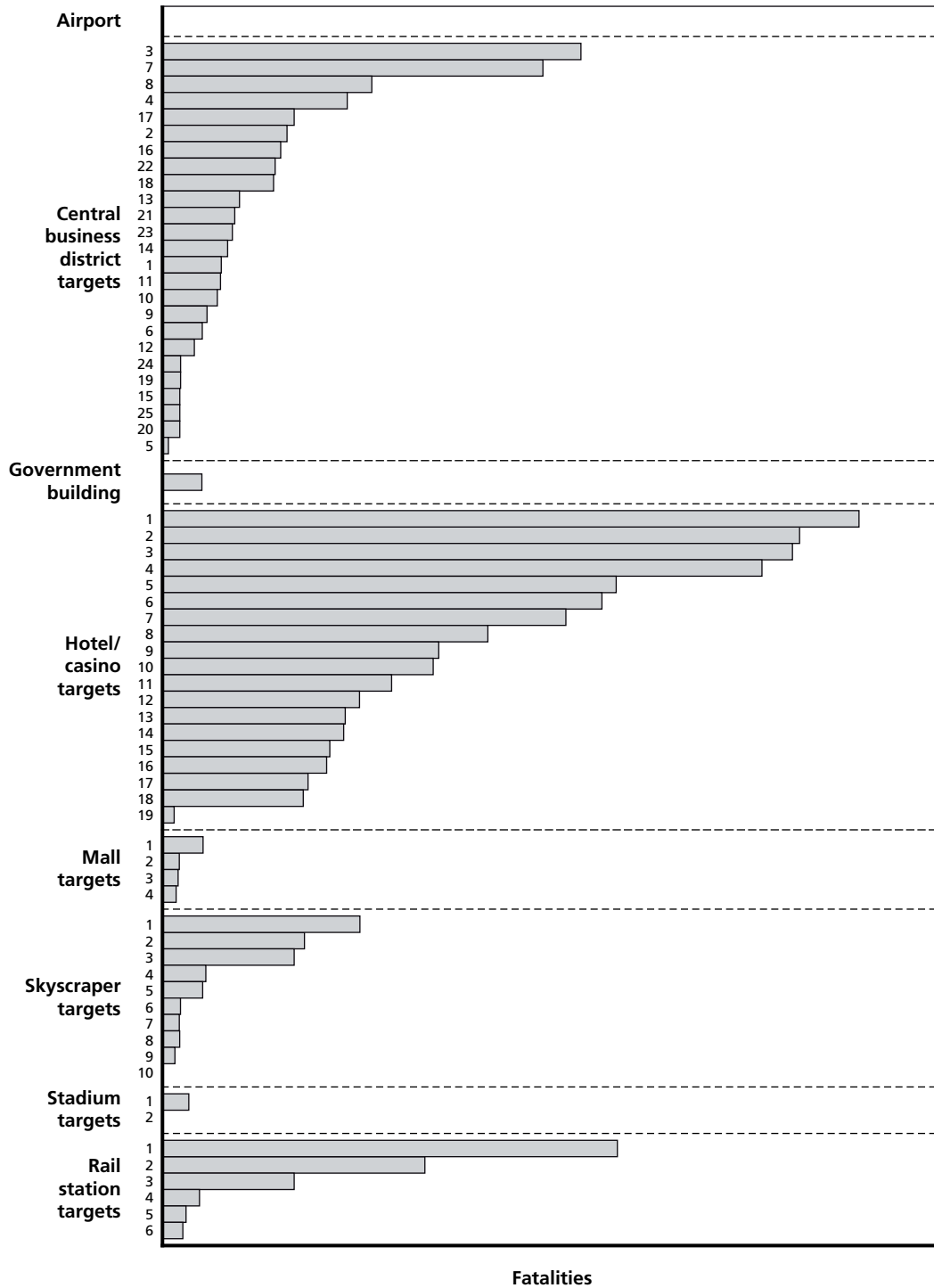
As discussed in Chapter Two, the occupancy of the hotel-casinos in the RMS model includes employees only and does not include hotel guests. Similarly, occupancy of businesses or airports would not include customers or passengers. Thus, potential fatalities for many targets, including hotels and airports, in Figure 4.3 are minimum estimates. Two of the central business districts also have potentially high fatalities, although the rest have much lower estimated consequences. Higher fatality estimates primarily reflect higher densities of people. Although bomb attack consequences are also influenced by building construction and other characteristics, most large structures in Las Vegas are relatively new and have similar susceptibilities to bomb blasts. Another important measure of the consequences of a terrorist attack is property damage. All property loss estimates presented in this report include damage to buildings and building contents only. Business losses and losses due to infrastructure interdependencies are not included in these data. Figure 4.3 shows the estimated property losses for the same 68 600-lb bomb scenarios.

In the case of property losses the hotel-casinos stand out even more markedly than for fatalities, reflecting the very large investments in commercial real estate along the Las Vegas strip relative to the central business districts.

We next examine the effect of the weapon type on attack consequences. Figure 4.4 shows the estimated fatalities for a 1-ton bomb attack at the same 68 targets examined in the 600-lb bomb case. In the case of a 1-ton bomb, there is less difference between the estimated consequences for hotel-casinos and central business districts. This reflects the fact that larger bombs have greater damage footprints, and therefore a larger fraction of the damage is incurred in surrounding areas. Most large hotel-casinos in Las Vegas are physically separated, while buildings in the central business districts are effectively contiguous, so the larger footprints of larger bombs produce more collateral casualties in business districts than in hotel-casinos.

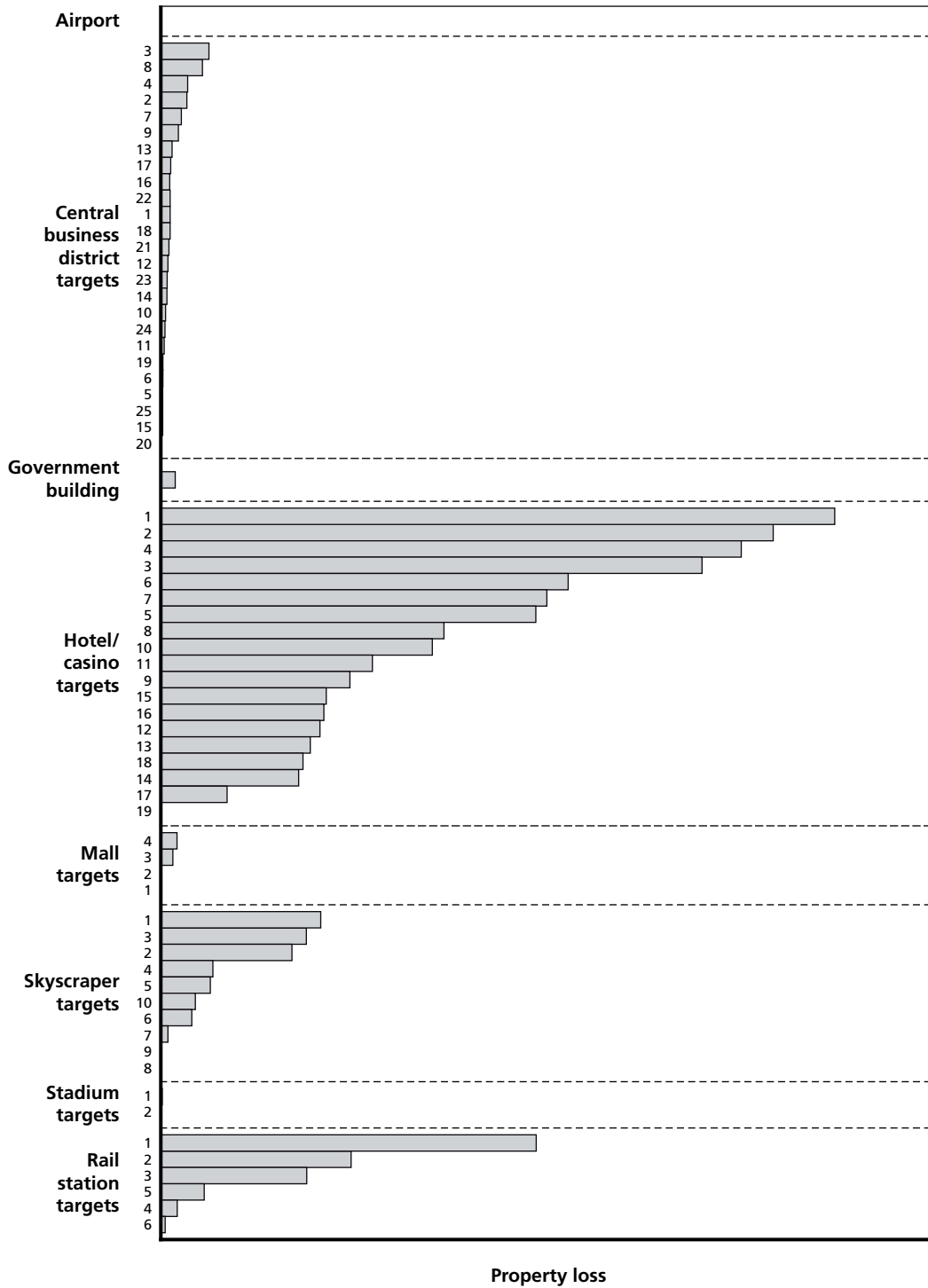
Figure 4.5 shows the corresponding potential property loss for the 1-ton bomb attacks. As with the 600-lb bomb case, estimated property losses for hotel-casinos are far greater than those for central business districts. Thus, while the difference between the estimated number of fatalities in hotel-casinos and those in central business districts decreases with increasing bomb size, estimated property losses are always much greater for the hotel-casinos. This indicates that identifying and ranking targets and target types susceptible to terrorist attack losses depends on the consequence metric used and details of the attack mode being considered.

**Figure 4.2**  
**Fatality Estimates for a 600-lb Bomb Attack on Targets in Las Vegas**

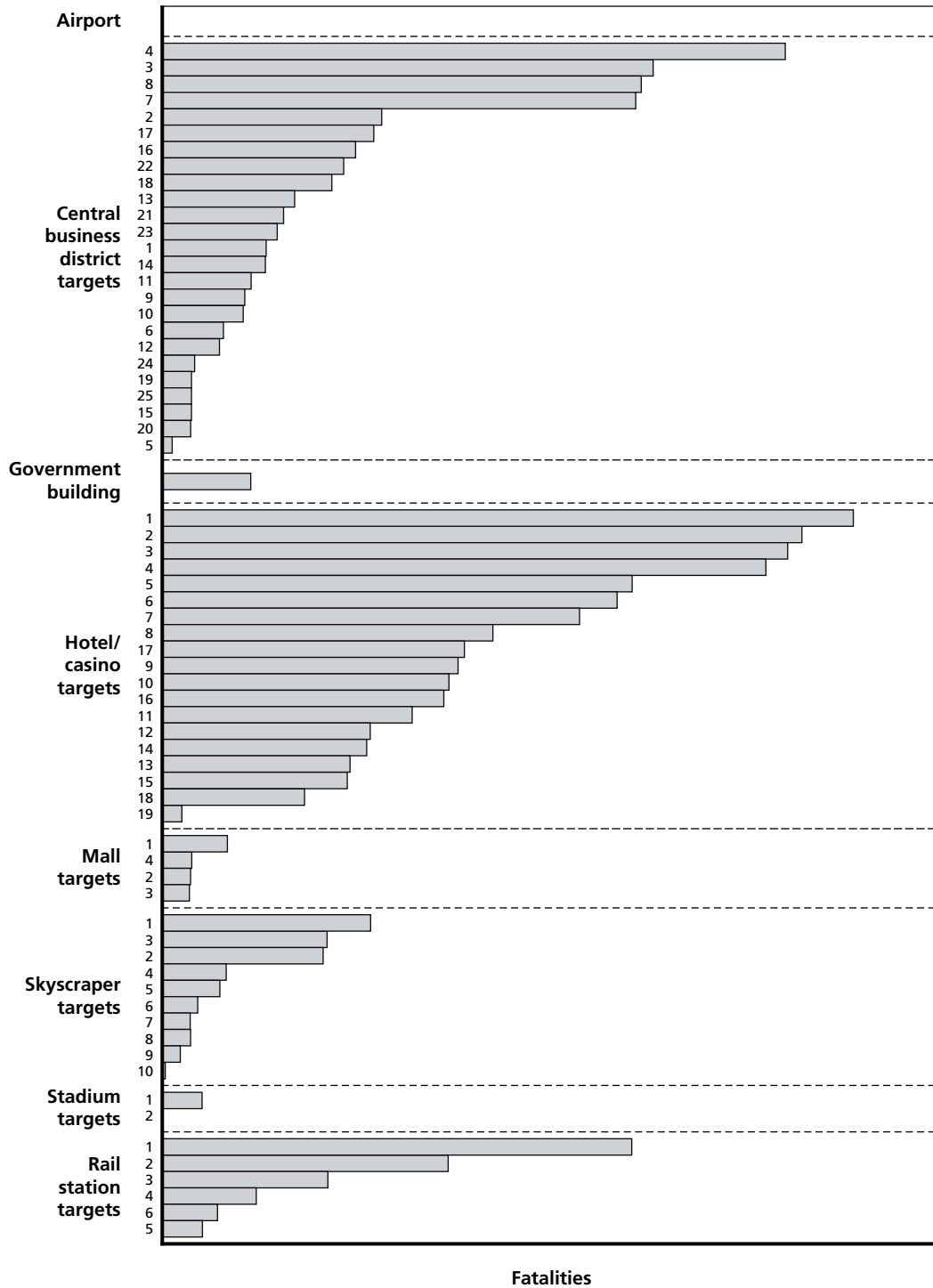




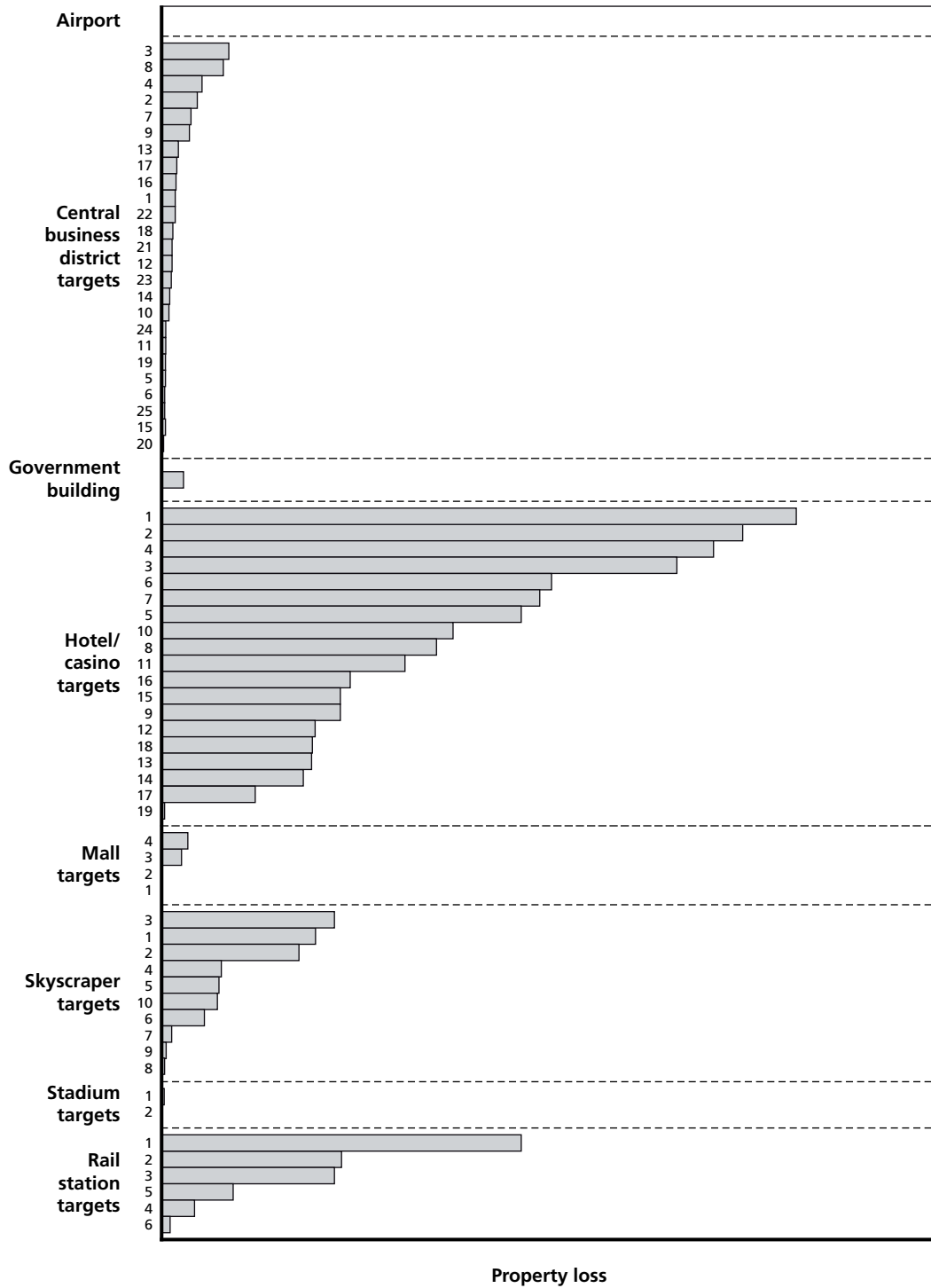
**Figure 4.3**  
**Property Loss Estimates for a 600-lb Bomb Attack on Targets in Las Vegas**



**Figure 4.4**  
**Fatality Estimates for a 1-Ton Bomb Attack on Targets in Las Vegas**



**Figure 4.5**  
**Property Loss Estimates for a 1-Ton Bomb Attack on Targets in Las Vegas**



## Terrorist Attack Risk in Las Vegas

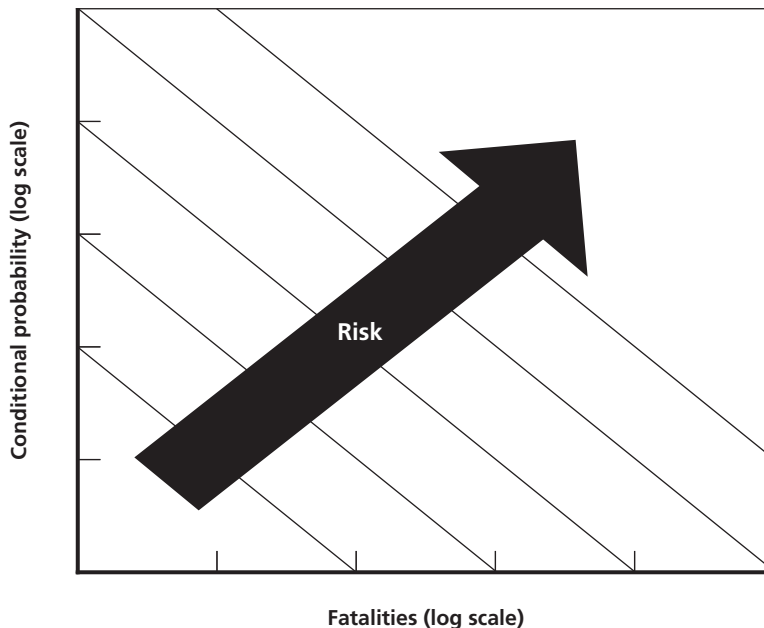
Risk reflects threat, vulnerability, and consequence. It is therefore a useful parameter for considering how to invest homeland security resources.

Risk can be examined along several dimensions to help guide decisionmaking. Risks can be compared among different locations, attack modes, and target types. Risk will also vary depending on what consequence measure is being considered (e.g., fatalities versus property loss). A useful framework for examining risk, illustrated in Figure 4.6, is to plot the consequences of an attack versus the probability of that attack occurring successfully. In this representation, contours of equal risk run from the upper left to the lower right (thin lines), and risk increases to the upper right, as shown by the arrow.

### Variation in Risk by Target Type

We first examine risk as a function of target type. Figure 4.7 shows the estimated risk, expressed in terms of fatalities, of attacks on the eight highest-risk target types in Las Vegas. Each point is a different attack scenario, where a scenario represents the pairing of a particular attack mode and a specific target. Shopping centers, oil refineries, and the airports tend to have the lowest risks in Las Vegas. In the case of airports and oil refineries, this is because, even in scenarios in which the RMS assessment considers threat to be relatively high, the expected fatalities in these scenarios are assessed to be relatively low. In the case of shopping centers, expected fatalities in successful attacks tend to be higher than in airport and oil refinery scenarios; however,

**Figure 4.6**  
Framework for Examining Terrorist Attack Risk



the probability of attack is assessed as being proportionally lower, so all these scenarios represent roughly the same level of risk.

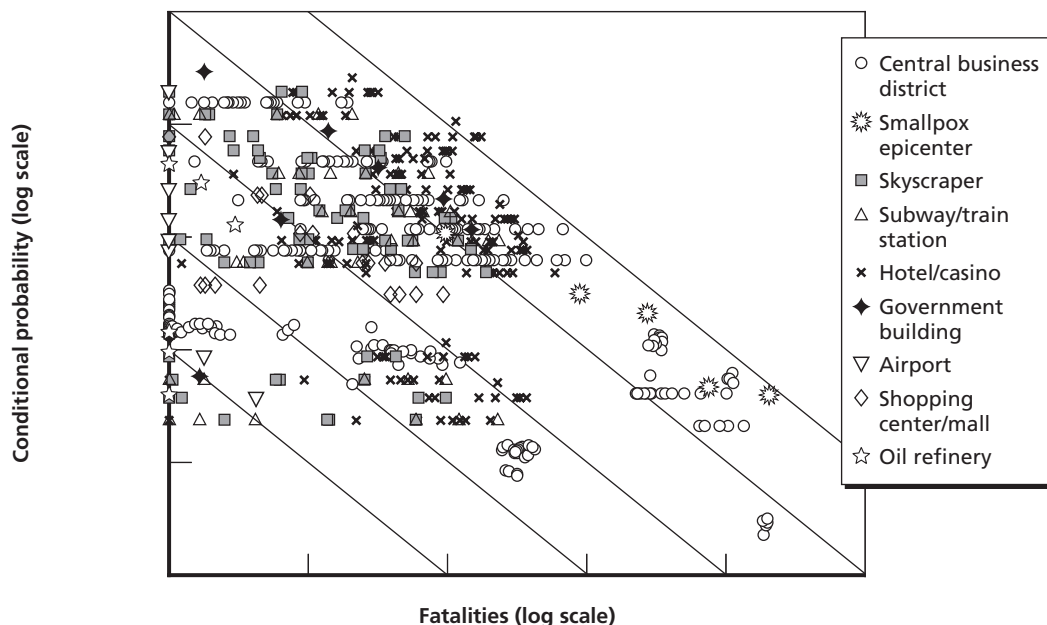
Only one government building is modeled in Las Vegas (Las Vegas's city hall). Despite the RMS model assigning government buildings the highest attack probability of any target type for a given attack mode, the consequences at city hall are relatively low, leading to only a moderate risk.

The RMS model assessment of government buildings being the highest-threat targets may not reflect the opinion that a terrorism threat in Las Vegas would be focused on casinos. This is a result of the RMS model not always reflecting interactions between target types and cities. As discussed later in this chapter, these assumptions can be changed to give hotels and casinos more importance in threat calculations to assess how estimated risk would change.

As noted previously, hotel-casinos are in the second highest target type attack likelihood tier modeled. Also, as noted previously, hotel-casinos suffer among the greatest potential fatalities for bombing attacks. Consequently, hotel-casinos have relatively high estimated risk for most attack modes. The risk estimates for subway stations in Las Vegas are comparable to those for hotel-casinos, because many stations are collocated with hotel-casinos. Most skyscrapers are lower risk than hotel-casinos. However, as noted previously, some skyscrapers are specific towers of some hotel-casinos, in which case their risk is also similar to that of hotel-casinos.

Finally, central business districts tend also to have high attack risk. Relative to hotel-casinos, the risk in central business districts is weighted toward lower-probability, higher-consequence events, which comprise primarily nuclear and large outdoor biological attacks.

**Figure 4.7**  
Fatality Risk for Terrorist Attacks on Different Target Types in Las Vegas

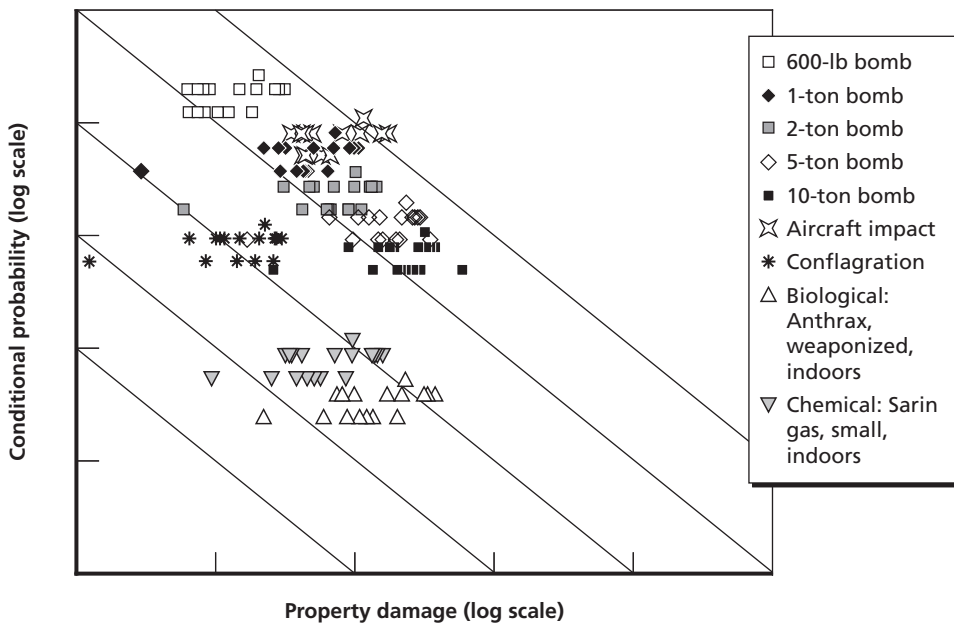


### Variation in Risk by Attack Type

Another important dimension of attack risk is attack type. Given the high overall risk and high visibility of hotel-casinos in Las Vegas, we examine the effect of attack type on hotel-casinos. Figure 4.8 shows the fatality risk for all scenarios involving hotel-casinos. Again, each point represents a separate scenario, where scenarios are now distinguished by attack mode. Risks for different attack types plot as clusters, where each cluster is made up of the individual hotel-casinos modeled. The positions of the clusters for the different-size bomb attacks illustrate the codependence of risk on both probability and consequence. Six-hundred-pound bombs have the highest probability but the lowest estimated consequences and therefore plot to the upper left. As the bomb size increases, the attack probability decreases and the potential consequences increase such that all different-size-bomb attacks plot along a trend parallel to the risk contours and therefore have similar risks.

Aircraft impacts have a risk slightly higher than that for the bombs, while the conflagration risk is lower. More specialized attacks involving sarin or anthrax have substantially lower probabilities and lower overall risk. Interestingly, probabilities aside, a large conventional bomb is expected to produce as many or more fatalities than an indoor chemical or biological attack. Note that the potentially very high consequence of outdoor biological and nuclear attacks are not modeled for hotel-casinos.

**Figure 4.8**  
**Fatality Risk for Terrorist Attacks Using Different Attack Modes at Hotel-Casinos**



### Variation in Risk by Consequence Measure

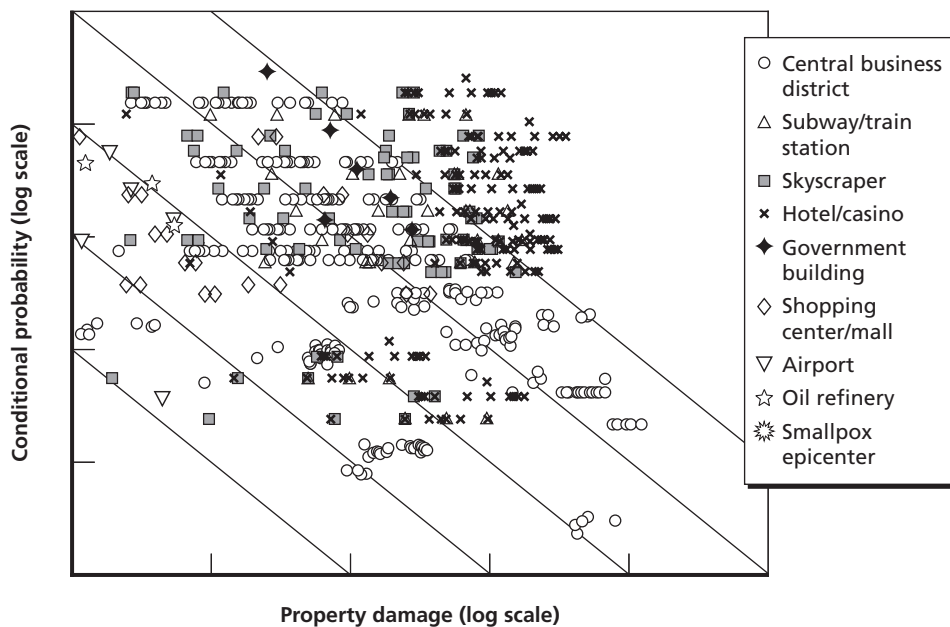
It is also useful to examine terrorist attack risk according to different consequence measures. Figure 4.9 shows the risk, this time expressed in terms of potential property loss, for all attack scenarios in Las Vegas. Compared to the fatality risk (see Figure 4.7), the large hotel-casinos (and associated subway stations and skyscrapers) stand out even further among the other target types. This perspective emphasizes the very high property values of the major hotel-casinos in Las Vegas.

### Spatial Variations in Risk

Finally, the RMS model provides a valuable way to examine spatial variations in risk. Figure 4.10 shows an illustrative example of the expected AAL of property over the hotel-casino strip (lower cluster) and central business district areas (upper cluster) in Las Vegas. AAL is a measure of risk, or the probability-weighted loss. The geocoded structure of the RMS model readily facilitates geographic information system depictions of model results.

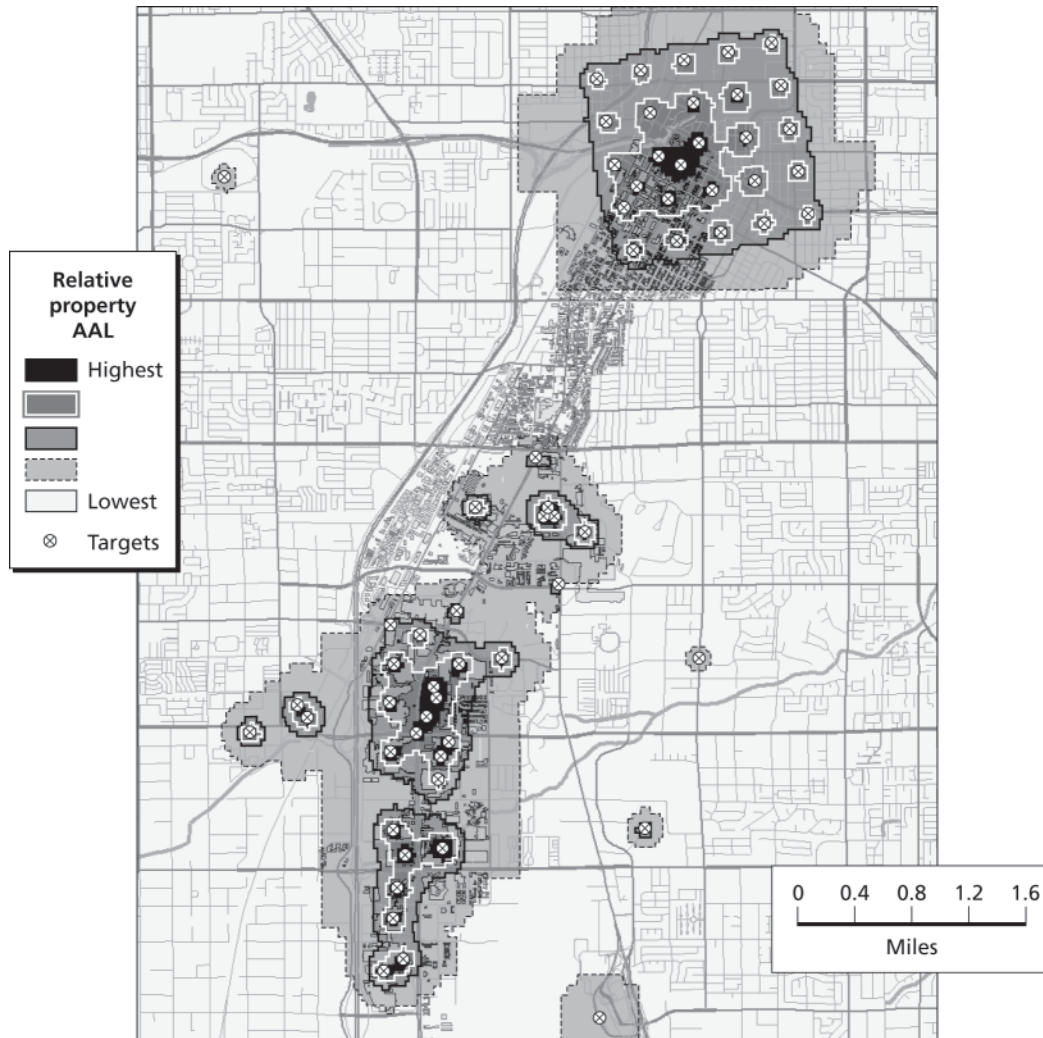
Estimated property losses are highly concentrated at the target points, although estimated losses from dispersal attacks, such as outdoor CBRN attacks, can extend for some distance from the target. Mapping expected losses provides another perspective on the distribution of expected consequences that could be useful for gathering intelligence or evaluating protection and response options. For example, Las Vegas is unusual in that the central business

**Figure 4.9**  
Property Loss Risk for Terrorist Attacks on Different Target Types in Las Vegas



RAND TR386-4.9

**Figure 4.10**  
**Distribution of Average Annual Loss of Property in Las Vegas**



SOURCE: RMS (undated).  
 RAND TR386-4.10

districts are geographically separate from the high-occupancy, high-value hotel-casinos in the strip area.

### Using Intelligence to Constrain Risk Estimates

In this section, we explore how the RMS model can be tailored with specific intelligence to constrain the risk profile for Las Vegas. This general approach is described in more detail in Chapter Five and is also demonstrated in Appendix D.

The approach entails comparing the estimated logistics capability of terrorist groups in past attacks to the logistics burden for different attack modes as defined in the RMS model. The logistics burden is a resource cost associated with each attack mode that represents the



**Table 4.1**  
**Logistics Capability Estimates for Past Hotel Attacks**

Logistics Component	Terrorist Capability Derived from OI&A Hotel Attack Scenarios	Capability Category from the RMS Model
No. personnel	14 to 16	10 to 15
Skill level	Capable of 400 to 1,300 lb vehicle-borne improvised explosive device	Advanced guerrilla tactics
Financing	\$50k to \$70k	\$50k to \$100k
Time	6 to 12 months	6 to 12 months

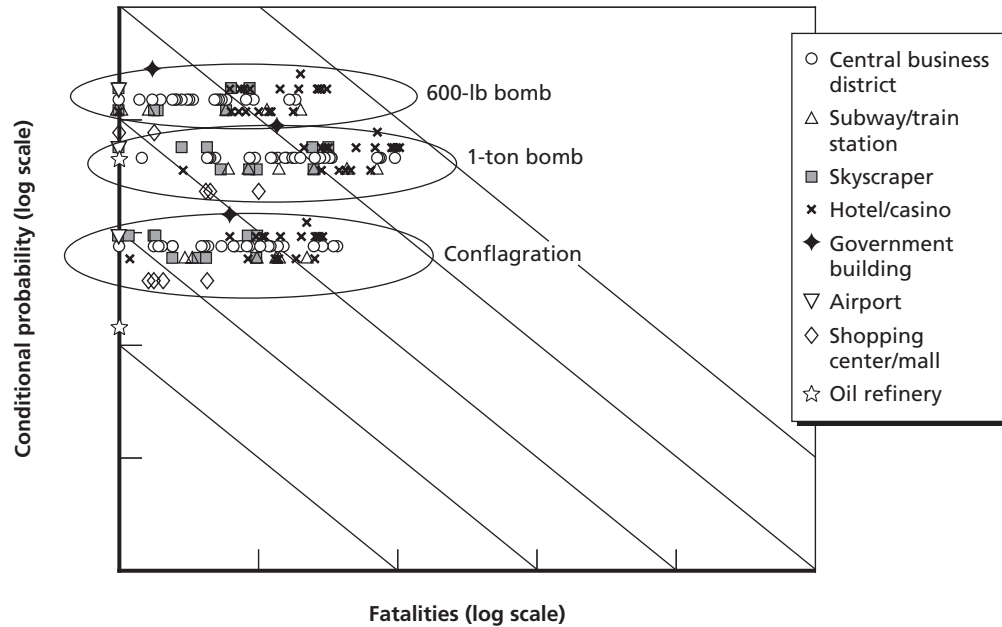
minimum capability required to be able to carry out that particular attack mode successfully. The logistics burden is defined in terms of four components, shown in the first column of Table 4.1: number of personnel, skill of personnel, money, and time.

Estimates of the logistics capabilities for terrorist groups that have attacked hotels in the past were derived from information collected in conjunction with hotel attacks in Kenya, Morocco, Indonesia, and Egypt. OI&A provided profiles of the terrorist groups that carried out the attacks, and we used these profiles to estimate values for each of the four logistics components used in the RMS model. The second column in Table 4.1 shows estimates of the values for each logistics component that we have determined from the profiles. Note that there are some gaps in the terrorist group profiles and therefore substantial uncertainties in the capabilities inferred from these profiles. In general, these estimates will be lower bounds, as unidentified personnel, money, and planning time are not accounted for.

As discussed in detail in Chapter Five, the RMS model groups individual component logistics values into discrete categories. The third column in Table 4.1 lists the component category from the RMS model that best matches the capabilities estimated by OI&A.

The logistics capabilities in Table 4.1 can be compared to RMS estimates of the logistics burden for various attack modes to constrain the types of attack that would have been within the capability of the terrorist groups that carried out the previous hotel attacks. Of the 37 attack modes in the RMS model, only five are estimated to be within the capabilities of these groups: small bombs (600 lb and 1 ton), surface-to-air missiles, conflagrations, and small sabotage with explosion and chemical release. The types of targets in Las Vegas further constrain this list, because two of the attack modes do not apply to the targets modeled in Las Vegas. The only industrial facility targets modeled in Las Vegas are oil refineries, for which a toxic release is not modeled. In addition, surface-to-air missile attacks are not associated with any particular location in the RMS model and therefore are not modeled in Las Vegas. This leaves three modes—600-lb bomb, 1-ton bomb, and conflagration—that are within the terrorist capabilities and possible in Las Vegas. The risk profile for this constrained list of attack modes is very different from the profiles presented previously. Figure 4.11 shows the fatality risk for the three potential attack modes, with different attack modes enclosed in separate ellipses. Comparison of Figures 4.12 and 4.8 shows that filtering available attack modes, based on terrorist capability profiling, limits the risk to relatively high-probability, low-consequence events. Low-probability, high-consequence events are excluded. The radical difference in the array of

**Figure 4.11**  
**Fatality Risk for Terrorist Attacks in Las Vegas for a Limited Selection of Attacks**



RAND TR386-4.11

possible scenarios between the unfiltered and filtered attack mode cases indicates that terrorist attack risk is highly dependent on assumptions about terrorist group capabilities.

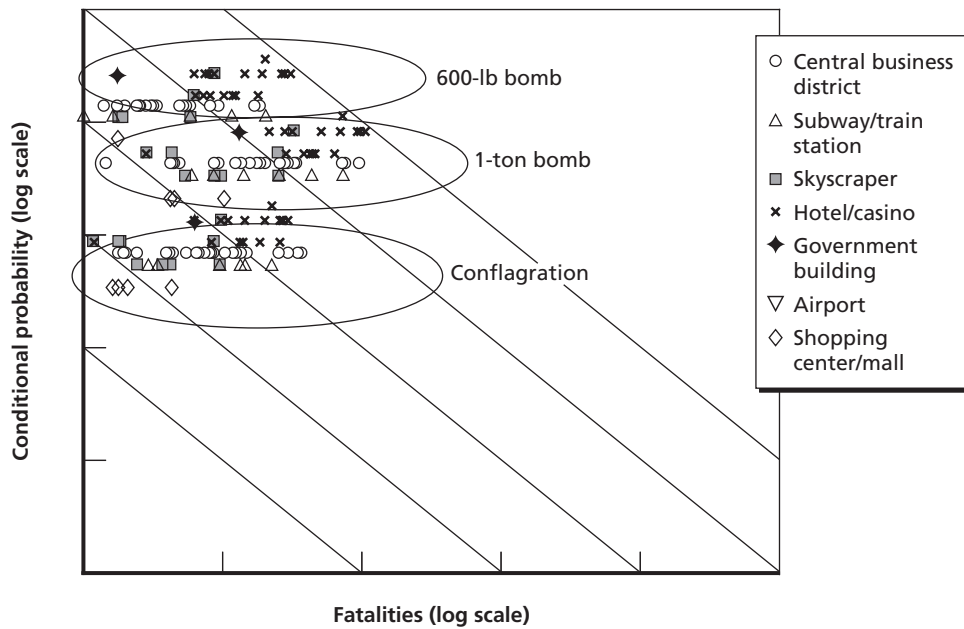
#### Effect on Risk of Increased Probability of Attacks on Hotel-Casinos

As noted in Chapter Three, the RMS model assigns the same relative likelihood of attack to a hotel in Las Vegas as it does to a hotel in any other city. However, a hotel-casino can be considered an iconic target type in Las Vegas and, if so, may be the most attractive target type in Las Vegas. To explore the effect of this possibility, we have conducted a sensitivity analysis to examine the effect of increasing the relative likelihood of hotel attacks in Las Vegas. For this analysis, we raised the target type relative likelihood of all hotel-casinos to tier 1. Likelihoods for all other target types were not changed. Changing the tier of the target allocates more terrorist risk to hotels based on their being assumed to be more attractive to terrorists.

Within the model, this increases their relative likelihood. The increased probabilities for hotel-casinos are shown in Figure 4.12. Because likelihoods are normalized (i.e., the overall probability of attack has not changed), the probabilities of most other target types have also decreased slightly. Comparison with Figure 4.11 shows that the difference, while noticeable, is relatively small compared to the overall range of risk among different scenarios.

As noted previously, filtering attack modes based on profiling the capabilities of terrorist groups is subject to uncertainty resulting from incomplete or inaccurate information. In this example, it is important to reiterate that the profiles provide only a minimum capability estimate; it is possible that the groups that carried out these attacks had access to more resources and were capable of conducting larger, more sophisticated attacks. In addition, we

**Figure 4.12**  
**Risk Profile for Terrorist Attacks in Las Vegas for a Limited Selection of Attack**  
**Modes and Hotel-Casinos Raised to Target Type Tier 1**



RAND TR386-4.12

have restricted our profiling to previous hotel attacks. Terrorist groups that have mounted larger attacks on other target types could easily target a hotel in the future.

## Summary and Conclusions

According to the RMS model, Las Vegas has the ninth highest overall terrorist attack probability in the country based on the city tier, number and types of targets available, and the attack modes possible for those attack types. Hotels and central business districts are the highest-risk targets. For 600-lb bombs, hotels are at the highest risk for potential fatalities, while, for larger bombs, hotels and central business districts have comparable risks. Aircraft impacts are the highest-risk events, followed closely by bombs and outdoor anthrax and smallpox attacks. The high estimated risk for aircraft impact attacks does not match terrorist patterns dominated by bombings prior to and since 9/11. In terms of property loss, the large hotel-casinos in Las Vegas have the highest risk for all attack modes. The risk profile derived by focusing only on attack modes estimated to be within the capability of terrorist groups that have conducted past attacks on hotels is strongly skewed toward relatively high-probability, low-consequence scenarios.

This case study demonstrates how the RMS model provides a quick survey of the nature and relative magnitude of terrorism risk in a specific urban area. This type of assessment can be used to develop terrorism risk profiles for other urban areas and could complement

knowledge that local officials have of their jurisdictions. Similar assessments to this analysis could be conducted for major metropolitan areas across the United States. They would provide a set of analyses that describes terrorism risk in common metrics and results from a consistent set of assumptions and application of data sets. The result would be summaries that could be readily compared. These analyses might prove useful for the federal government when assessing the implications of newly obtained intelligence. For example, if faced with analysis that suggested that threats to hotels were elevated, an analysis like this could be used to identify urban areas where changes in assumptions about the threats to hotels would mean the largest increases in risk to the urban areas. In some cases, this information could be used to deploy additional law enforcement or recommend modifying operations in response to the threat.

It could also be useful in evaluating what the greatest needs are for a particular community and in helping to justify the use of federal preparedness grant funding for specific types of projects. For example, when applying for federal grants to make Las Vegas safer, this analysis can help differentiate risks between the strip and the downtown area. Understanding how the nature of risk varies by target type and attack mode throughout a community could help assure that funds are directed toward projects that reduce the greatest risks.<sup>2</sup>

---

<sup>2</sup> The goal of risk reduction should be to direct funds toward projects that achieve the greatest risk reduction per dollar, within certain reasonable constraints. This project does not attempt to do this cost-benefit analysis.

## Application 3: Informing Threat Assessment Using the RMS Terrorism Risk Model

---

In developing useful intelligence products for state and local officials, OI&A must translate available intelligence coupled with vague statements of terrorists' intentions and capabilities into directives of what types of event to look for, when, and where. In other words, the goal of intelligence analysis is to translate raw intelligence and other information into actionable intelligence.

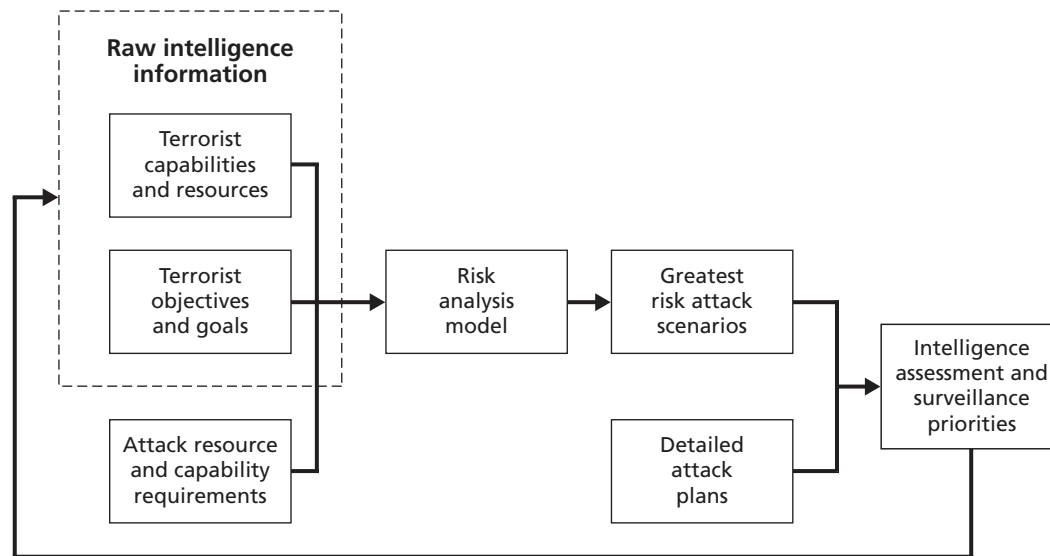
In this chapter, we discuss how risk-analysis tools may help support intelligence collection and analysis. The RMS model is used as an example of risk analysis used in the insurance industry. This chapter refers to the RMS model to illustrate how this tool could be considered for an application very different from that for which it was originally developed: informing intelligence analysis and collection requests at OI&A.

### Overview of Approach

A major city may be vulnerable to thousands of different potential terrorist attacks. If the resources required to accomplish different attacks can be characterized, if some insight into terrorist capabilities can be collected, and if the consequences of different attacks can be related to terrorists' goals, then the full set of possible attacks could be reduced to only those for which the terrorists' capabilities meet or exceed the attack requirements and for which attack consequences correspond to their goals. The basic approach thus entails comparing terrorists' intentions, capabilities, and resources with the resource requirements and consequence estimates for various possible attacks in an attempt to constrain the range of probable attacks and, ultimately, to help guide intelligence analysis and surveillance efforts.

The inputs to intelligence analysis, shown on the far left in Figure 5.1, are imperfect intelligence information, including tactical information and indications of terrorists' intentions and capabilities. Together, terrorists' intentions and capabilities determine what attacks will be attempted to achieve the groups' goals and objectives. Intelligence about terrorists' intentions implies limits on what terrorists are likely to attempt to reach goals, since some attack modes will not accomplish consequences that support these intentions. Intelligence about terrorists' capabilities implies constraints on what terrorists could possibly accomplish. Terrorist objectives and goals may influence preferences for attack modes, target types, or targeted cities

**Figure 5.1**  
**Approach for Incorporating Risk-Analysis Tools into the Intelligence Process**



RAND TR386-5.1

Required capabilities and resources for different types of attack can be determined by considering specific attack scenarios. In the case of the RMS model, public source information was used to estimate the logistics burden of the 37 attack modes modeled. These resources are defined in terms of the number and skill level of personnel, capital expenditures required, and time needed for planning. Specifically, the model characterizes resources using the following metrics and descriptions:

- skill level and personnel requirements
  - Volunteer or practical skills: The attack can be carried out using only manual labor or school-educated personnel.
  - Basic terrorism skills: The attack requires military training skills up to basic combat level, including the ability to handle personal weapons and carry out close-quarter combat.
  - Advanced guerrilla tactics: The attack requires accurately positioning explosives, firing accurately, or using more sophisticated military weapons.
  - Extramilitary skills: The attack requires a specialist or professional in a particular skill to carry out, such as a computer hacker, a qualified airline pilot, or a person with relatively rare manufacturing or production skills.
  - Specialized skills: The attack requires specialized skills, such as a physicist, chemist, or biological scientist capable of operating sophisticated equipment and carrying out hazardous processes safely.
  - Highly specialized skills: The attack requires highly specialized and rare skills, such as a qualified operator of a nuclear power plant or a large-scale manufacturing or high-precision production operation in secret.

- number of personnel involved in planning and execution, ranging from one to more than 50
- capital requirements, ranging from less than \$1,000 to \$5 million
- time needed to plan and implement, ranging from less than one month to more than five years.

There is a wide range of values for each of these factors when considering the 37 attack modes modeled. The assumptions laid out are well documented. However, as with all parameters in the model, they require sensitivity analysis when used to generate results. Appendix D provides an example of how the RMS estimates of required capabilities for different types of attack can be used to focus intelligence analysis and collection on attack modes that most closely correspond to intelligence estimates of terrorists' suspected capabilities.

Risk-analysis tools, such as the RMS model, can be used to analyze raw intelligence to help understand what attack modes meet terrorists' objectives in terms of consequences, required capabilities, and available skills and resources. In other words, the RMS model could use intelligence information to provide an estimate of the attack scenarios that represent the greatest risk.

This set of high-risk attack scenarios can help inform and focus intelligence assessments and surveillance efforts. Ideally, OI&A intelligence assessments could generate output in the form of actionable intelligence that can be used by law enforcement (or the military) to prevent future terrorist attacks and to apprehend or kill terrorists. However, the set of high-risk attack scenarios that is produced by the RMS model would be more valuable if augmented with more detailed tactical-level information about where terrorists are likely to strike and what specific activities are indicative of attack planning.

To reach the desired greater level of resolution, intelligence analysts would combine a set of high-risk attack scenarios with detailed characterizations of the activities and timelines that correlate to the different types of terrorist attack scenarios. DHS, local law enforcement, and others may already have this type of information. Together, these two types of information could be combined to produce specific intelligence that points to specific targets, attack modes, and times. The information could also be used to refine surveillance priorities to collect additional information on terrorist activities.

While using terrorism risk modeling in this way could make intelligence collection and analysis efforts more effective, it would be unwise for intelligence collection efforts to focus exclusively on threats identified through this process. There may well be adversaries about which we do not know or threats that have not yet been envisioned. As discussed later in this chapter, the proposed approach may be able to narrow searches among threats that are known but is not designed to help prevent failures of imagination.

### **Can Intentions Be Matched with Outcomes?**

One challenge of this approach is translating concepts of terrorists' intentions into quantifiable outcomes as measured in the RMS model, such as injuries, fatalities, or economic damages. In the National Infrastructure Protection Plan (NIPP), developed in support of Homeland



Security Presidential Directive 7 on Critical Infrastructure Identification, Prioritization, and Protection, DHS has used similar translations of event consequences to prioritize terrorism scenarios (DHS, 2006). In the NIPP, the prioritization was based on how U.S. values should guide defensive priorities. In this case, the translation would be meant to reflect values of terrorists.

Intelligence collection efforts may develop varied sources of information about terrorist goals, intentions, resources, and capabilities. This includes reviewing writings and recordings or developing case studies of both successful and known disrupted attacks. OI&A provided access to case studies for a number of past attacks developed by the New York City Police Department (NYPD). These sources generally identify broad goals, such as killing Americans or damaging the U.S. economy. The RMS model, on the other hand, estimates consequences of specific terrorist attacks in terms of fatalities, injuries, and economic damage. Translating broad statements of intentions into specific outcomes continues to be a major challenge for the intelligence community.

Terrorism experts at RAND and elsewhere consider these questions when reviewing intelligence information in an effort to develop guiding principles that may help link intentions to outcomes. For example, small events may not have large enough effects to motivate terrorists. Alternatively, events that are too large may create a negative backlash. Logic to close the gap between intentions and outcomes is not contained in the RMS model—it will need to be obtained from other sources and incorporated into a broader analytic approach. Any information that the intelligence community has on translating between broad intentions and event outcomes can be used to refine risk estimates from the RMS model by providing an indication of higher-probability attack mode–target combinations.

### **Options for Refining This Analytic Approach**

Progressing with this research raises three paths for discussion. The first path addresses how to make this analytic approach most beneficial for DHS. Which aspects of the approach presented in this chapter seem most useful? Are classified or unclassified results more useful? Should other DHS elements be included in the formulation of analysis or briefings of methodology and results? The best way to answer these questions is for OI&A to exercise this process as a tool for analysis.

The second path addresses how to improve the model through the use of better information. Specifically, in the example presented in Appendix D, the RAND team relied on input derived from NYPD case studies rather than on actual statements about terrorist organization capabilities and intentions provided by the intelligence community. Additionally, working with the intelligence and law enforcement communities to define and refine the desired output of the model would result in an improved approach and product.

The final path involves comparing this work to other methods used. In continuing work, the approach described in this section could be compared to analysis done by OI&A using independent means. A series of exercises (or even a single exercise) with OI&A and other agencies using this and other models would help DHS understand the comparative value of differ-



ent models as tools for intelligence analysts. In these exercises, agencies could work together or could independently translate assessments of a terrorist group's intentions and capabilities into parameters the RMS model can use. The results could then be used to assess terrorism risk in a major urban area to see what attack mode–target pairs are most aligned with these threat assessments. Finally, a few of these attack mode–target pairs could be deconstructed to determine what specific indicators might be suggested to be worth exploring with the intelligence and law enforcement communities.



## Conclusions and Recommendations

---

This project looked at three different ways in which terrorism risk models and the RMS model in particular could be used to assist OI&A, DHS more broadly, and the larger community responsible for homeland security. These three distinct, though complementary, approaches yield different lessons that could help secure the United States from terror attacks. These lessons were presented in each of the three preceding chapters and are consolidated and expounded on here.

### Using Terrorism Models to Assess Risk Across Cities

In Chapter Three, we considered the risk to terrorist attack in UASI areas and performed a comparative analysis of these findings. The most important conclusions are that most of the nation's risk from terrorist attacks resides in a small handful of cities (most of the UASI cities have relative risks that are significantly lower than the risk experienced by this handful of high-risk cities) and that the percentage risk from different types of attack makes risk management and resource allocation an effort that requires detailed information about the risk profile of each city (see preceding discussion).

This analysis addressed three questions posed by HITRAC:

1. How is terrorism risk distributed across UASI cities?
2. Is the distribution of RMS's terrorism risk estimates different when measured as property risk versus fatality risk?
3. How does the distribution of RMS risk estimates differ by attack mode?

For this analysis, we considered a slightly modified version of the UASI list of cities (see Appendix C) and three categories of attacking them: conventional means, CBRN, and sabotage. Analysis was based on comparing risk for each type of attack with the aggregate risk across cities. Risk was calculated overall and separately for fatalities and property loss, and the results were compared. Risk is presented as "risk shares," which represent the percentage of national risk in each city.

The fundamental conclusion of this analysis is that according to the RMS model, terrorism risk is concentrated in a small number of UASI-eligible cities, with most cities having negligible relative risk. For example, considering fatalities only, New York accounts for most of the

national risk, with the next closest city being Chicago. 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. Interestingly, Washington and the capitol region appears to have a disproportionate share of terrorism risk compared to the region's population, but the share of UASI allocations exceeded the share of estimated terrorism risk.<sup>1</sup> For all other urban areas, estimated terrorism risk shares fall below both the distribution of population and UASI allocations. This result does not change much when considering property loss. The average absolute difference between the property value and fatality risk shares was only 0.3 percent. The largest differences occur in the cities with the largest risk and range in magnitude from 1 percent to 3 percent.

More interesting is the analysis of how risk changes by attack mode. Here, there is some variability within each city regarding risk from conventional, CBRN, and sabotage attacks. Those few cities that do experience substantial changes with regard to CBRN do so for readily apparent reasons. For example, Jersey City, New Jersey, experiences a significant increase in CBRN risk, but this appears to be due to its proximity to New York City, with its high risk of CBRN attacks. Sabotage risk deviation from overall risk is even more pronounced and is due to the proximity of nuclear power plants, chemical plants, or oil refineries (the only types of facility considered with respect to sabotage) to each city. Cities without major facilities of these types are not significantly exposed to sabotage attacks. These differences are nicely summarized in Figure 3.6 in Chapter Three, which depicts the percentage of city risk from each type of attack. This figure provides city homeland security managers with an easy-to-understand depiction of their exposure to various types of risk. This analysis also highlights the value of considering different perspectives on risk. While this study has assessed only terrorism risk, UASI and other grant programs focus on natural disaster risk as well. Similar insurance-industry models of natural disaster risk could readily be incorporated into this type of analysis.

This case study also highlighted several paths to making the RMS model more useful for resource allocation decisionmaking:

- The model databases, particularly the target database, should be compared to other data sets and possibly expanded.
- The consequences model should be linked to other models of indirect economic effects to understand the relative importance of the consequences of interconnected infrastructure systems.
- These results should be compared to analysis using different assumptions about terrorist threats as well as different models, including those that address natural disaster risk.
- 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 to terrorism risk.

---

<sup>1</sup> Resource allocation has, in the past, been based in part on population.

## Recommendations

Analysis of the first 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 the insurance-industry models noted previously to improve the usefulness of this approach to homeland security analyses.

## Using Terrorism Models to Assess Risk Within Specific Cities

In Chapter Four, we presented an analysis of the terrorist threat in Las Vegas using the RMS model. This effort began with a description of how the RMS model ranks cities and with specific information about how targets are ranked. From that point, we analyzed and compared the relative likelihoods of and losses from different types of attack. We then presented the risk of different targets and target types from different types of attack and with respect to deaths and property losses. The figures that present this information (Figures 4.8 to 4.11) provide DHS and, more importantly, local decisionmakers, with an easy-to-understand graphical display that illustrates the probability, expected loss, and risk from different types of terrorist attack. Following this presentation, and similar to the approach discussed in Chapter Five, these graphics are overlaid with the types of attack that could produce the losses previously discussed and a presentation of the capabilities that terrorist groups would need to achieve these effects.

This presentation 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 in 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?

The answers to the first two questions are relatively straightforward (although the answer to the first question is more extensively addressed in Chapter Three). We note, however, that these questions are equally, if not more, important for local officials than for DHS. The discussion of attack mode likelihood (summarized in Figure 2.3 in Chapter Two) provides local homeland security officials with a wealth of useful information concerning the types of attack against which they should prepare to defend; for example, the threat from bombs and other conventional attacks is much higher than from CBRN attacks in certain cities. The information in the discussion of consequences (summarized in Figures 4.2 to 4.5 in Chapter Four) gives local officials an understanding of what the effects of such attacks might be. Finally, the information contained in the discussion on risk (summarized in Figures 4.6 to 4.11 in Chapter Four) 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 with a metric (i.e., expected fatalities or property losses) that provides an accepted default for making decisions on prevention and protection actions.

Of particular importance to DHS is the third question. Given intelligence about likely attacks of a specific kind (e.g., on hotels or casinos), the RMS model can be used to evaluate how the relative risk to Las Vegas changes when considering new information. One component of this analysis was undertaken as part of this study: We elevated hotels (a tier 2 target) to tier 1 status to simulate an increased threat. However, more could be done on the local level if the relative probabilities of targets and attack modes were reevaluated based on intelligence. For example, the information produced by the RMS model could be used in tasking intelligence and law enforcement assets to counter specific threats to casinos and resort hotels.

In general, this analysis provided information about the risk from terrorist attacks in Las Vegas. In effect, it provides a city profile with distinct risk characteristics that could be used to 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.

Chapter Four also provides insights into potential extensions of the RMS model. One important capability of the RMS model is the ability to account for features of individual targets that 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 could be modified to 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 underused, 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. For the same reason, the model does not include stadium spectators or passengers in airport terminals and planes. 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. While the model provides seemingly useful results as developed, 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 security missions. Assuming that additional data of these types are available, accommodating them in the model will be straightforward.

Finally, as discussed earlier, the model assigns the same relative likelihood to all targets of a given type, regardless of their symbolic association with a particular city or other circumstances in which particular target types may have heightened relative likelihoods. Examples could include hotels in Las Vegas versus hotels in Pittsburgh; government buildings in Washington, D.C., versus government buildings in Las Vegas; or financial offices in New York City versus financial offices in Portland. We have explored the effect of relaxing this constraint in

this analysis by raising the relative likelihood of attacks on hotels in Las Vegas and find that it has a strong effect on the estimated risk for hotels in Las Vegas. Additional analysis with this model should allow for special considerations affecting relative likelihoods of target types or attack modes.

The RMS Probabilistic Terrorism Model provides some useful insights about terrorist attack risks that can help OI&A in its mission to analyze homeland security–related intelligence and other information to provide guidance and alerts to the nation about emerging terrorist threats. One very important aspect of the model is that it provides an analytical framework that translates structured discussions of intelligence and other information into a parameterized estimate of terrorist attack probability. In addition, it uses detailed modeling of weapon effects, engineering principles, and target-specific data to estimate the casualties and property losses for 37 attack modes and more than 3,000 targets across the United States. Taken together, probabilities and consequences provide an estimate of the terrorist attack risk (vulnerability is incorporated in the target-specific data), which can be examined according to geography, attack mode, target type, and estimates of terrorist capabilities and intentions.

Furthermore, the model appears well suited for comparisons at the national level (discussed below), where the combined effects of city, target type, and attack mode likelihoods provide the greatest resolution to compare the risk of individual scenarios. While consequence modeling is tailored to specific targets, attack likelihoods are not well distinguished at the individual target level, so risk comparisons within cities have some problems not encountered when comparing risk across cities.

### **Recommendations**

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 Terrorism Risk Models to Assist Intelligence Analysis**

In the third application, we incorporated the RMS model into the process typically used by OI&A analysts of 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 does two things. First, it identifies the specific targets and attack modes of greatest risk that meet terrorist goals. 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.

### **Recommendations**

Analysis of the third 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.



## RMS Terrorism Advisors' Network

---

Individual consultants who contributed to the development of the RMS Terrorism Risk Model include the following (items in *italics* indicate areas of expertise):

- **Rohan Gunaratna**, head of terrorism research, Institute of Defense and Strategic Studies, Nanyang Technological University, Singapore  
*Terrorism threat from Al Qaeda and associated groups*
- **Magnus Ranstorp**, director, Centre for the Study of Terrorism and Political Violence, University of St. Andrews, Scotland  
*Terrorism threats from Islamic militant groups and political violence in the Middle East*
- **Bruce Hoffman**, professor, School of Foreign Service, Georgetown University, Washington, D.C.  
*Terrorism risk in the United States*
- **K. Jack Riley**, associate director, RAND Infrastructure, Safety, and Environment, Pittsburgh, Pa.  
*Homeland security*
- **Robert Reville**, director, RAND Institute for Civil Justice; codirector, RAND Center for Terrorism Risk Management Policy, Santa Monica, Calif.  
*Terrorism compensation and liability*
- **Darius Lakdawalla**, economist, RAND Corporation, Santa Monica, Calif.; faculty research fellow, National Bureau of Economic Research  
*Probabilistic modeling and economics of terrorism risk*
- **Brian Chow**, senior physical scientist, RAND Corporation, Santa Monica, Calif.  
*Loss modeling and the defense and control of terrorism weaponry*
- **Greg Jones**, senior defense policy analyst, RAND Corporation, Santa Monica, Calif.  
*Chemical, biological, radiological, and nuclear weapons in terrorism*
- **George Zanjani**, economist, capital market function of the research and market analysis group, Federal Reserve Bank of New York  
*Economics of terrorism insurance*
- **Brian A. Jackson**, physical scientist, RAND Corporation, Arlington, Va.  
*Emergency response to terrorism incidents*
- **Kim Cragin**, international policy analyst, RAND Corporation, Arlington, Va.  
*Historical data on terrorism attacks*

- **Gregory Treverton**, senior policy analyst, RAND Corporation, Santa Monica, Calif.  
*Terrorism, intelligence, and law enforcement*
- **Lois Davis**, senior policy researcher, RAND Corporation, Santa Monica, Calif.  
*Defense and security at targets*
- **James Quinlivan**, senior analyst, RAND Corporation, Santa Monica, Calif.  
*System analysis research*
- **Pete Baxter**, director, global consultancy operations, Jane's Information Group, Alexandria, Va.  
*Attack technology, logistical burden, and red-teaming analysis*
- **Michael Dell**, director, Jane's Information Group  
*Terrorism intelligence and news analysis*
- **Mark Mateski**, consultant and project manager, Jane's Information Group  
*Red teaming, site security, and logistical burden*
- **David Kuhn** Jane's Information Group  
*Weapon systems and unconventional attack operations*
- **Charles Heyman**, editor, Jane's World Armies; senior military advisor, Jane's Information Group  
*Site security*
- **Paul Mahoney and Laura Dake**, Jane's Information Group  
*Security survey of New York skyscrapers*
- **Roger Davies**, Hazard Management Solutions Ltd.; editor of TRITON terrorist activity database, Faringdon, Oxfordshire, UK  
*Consultant on attack technology (RMS terrorism model 1.0), provider of data and reports (RMS terrorism model 2.0)*
- **William Kastenber**, professor, nuclear engineering, University of California, Berkeley; member, Advisory Committee on Nuclear Facility Safety, U.S. Department of Energy  
*Nuclear power plant safety against terrorist attack*
- **Rich Balzano**, consultant, Jane's Information Group  
*Nuclear power plant operations and security*
- **Lawrence M. Wein**, professor, management science, Graduate School of Business, Stanford University, Palo Alto, Calif.  
*Bioterrorism attacks and emergency response*
- **Mark Sauder**, consulting engineer  
*Industrial facilities vulnerability*
- **Malcolm Cowler**, senior engineering analyst, Autodyn  
*Use of computational fluid dynamics for blast modeling*

## City Tiers and Likelihoods from the RMS Probabilistic Terrorism Model

---

**Table B.1**  
**City Tiers and Likelihoods from the RMS Probabilistic Terrorism Model**

City Tier	City Names
1	New York, Washington
2	Chicago, Los Angeles, San Francisco
3	Boston, Houston, Las Vegas, Miami, Philadelphia
4	Cleveland, Detroit, San Diego, Seattle
5	Atlanta, Buffalo, Dallas, Denver, Orlando, San Jose, St. Louis, St. Petersburg, Tampa
6	Austin, Baltimore, Charlotte, Ft. Lauderdale, Ft. Worth, Minneapolis, Newark, Oakland, Phoenix, St. Paul
7	Cincinnati, Columbus, Hartford, Indianapolis, Jersey City, Kansas City, Long Beach, Milwaukee, New Haven, New Orleans, Norfolk, Pittsburgh, Portland, Riverside, Sacramento, Salt Lake City, San Antonio, Stamford
8	Honolulu

SOURCE: RMS (undated).



## Definitions of Fiscal Year 2005 UASI-Eligible Urban Areas

---

**Table C.1**  
**Definitions of Fiscal Year 2005 UASI-Eligible Urban Areas**

Urban Area	Defined Urban Area
Phoenix, Ariz.	City of Phoenix; Maricopa County, inclusive of the portions of Gila River Indian Community, Salt River-Pima Indian Community, and Fort McDowell Indian Tribe lying within Maricopa County
Anaheim/Santa Ana, Calif. <sup>a</sup>	City of Anaheim; City of Santa Ana; Orange County; cities of Cypress, Buena Park, Stanton, Garden Grove, Fullerton, Placentia, Yorba Linda, Tustin, Orange, Costa Mesa, Fountain Valley, and Irvine and unincorporated Orange County
Oakland, Calif.	City of Oakland; Alameda County; the Port/Airport, Berkeley, San Leandro, Alameda, Emeryville and Piedmont. Secondary area: entire counties of Alameda and Contra Costa
San Francisco, Calif.	City and County of San Francisco; counties of Marin, San Mateo; and the Golden Gate Bridge District
San Jose, Calif.	City of San Jose; County of Santa Clara; counties of Monterey, San Benito, and Santa Cruz; cities of Campbell, Cupertino, Gilroy, Los Altos, Los Altos Hills, Milpitas, Monte Sereno, Morgan Hill, Mountain View, Palo Alto, Santa Clara, Saratoga, and Sunnyvale; and town of Los Gatos
Los Angeles/Long Beach, Calif. <sup>b</sup>	City and County of Los Angeles; Los Angeles County Unincorporated; cities of Beverly Hills, Burbank, Carson, Commerce, Culver City, El Segundo, Glendale, Hawthorne, Inglewood, Pasadena, San Fernando, Santa Monica, Torrance, Vernon, and West Hollywood; City of Long Beach; cities of Bellflower, Carson, Compton, Hawaiian Gardens, Lakewood, Paramount, and Signal Hill
Sacramento, Calif.	City and County of Sacramento; West Sacramento; cities of Folsom, Roseville, Rocklin, and the southern portion of Placer County
San Diego, Calif.	City and County of San Diego, inclusive of cities of Carlsbad, Chula Vista, Coronado, Del Mar, El Cajon, Encinitas, Escondido, Imperial Beach, La Mesa, Lemon Grove, National City, Ocean-Side, Poway, San Marcos, Santee, Solana Beach, and Vista
Denver, Colo.	City and County of Denver; counties of Adams, Jefferson, and Arapahoe
Washington National Capital Region	District of Columbia; counties of Montgomery and Prince George's (Md.); counties of Arlington, Fairfax, Prince William, and Loudon (Va.); cities of Falls Church, Manassas, Manassas Park, Fairfax, and Alexandria (Va.)

**Table C.1—Continued**

<b>Urban Area</b>	<b>Defined Urban Area</b>
Jacksonville, Fl.	Duval County
Miami, Fl.	City of Miami; counties of Miami-Dade and Broward
Tampa, Fl.	City of Tampa; Hillsborough County; Pinellas County, inclusive of Clearwater, Temple Terrace, and St. Petersburg
Atlanta, Ga.	City of Atlanta; counties of Fulton and DeKalb, Georgia; supported by the contiguous counties of Gwinnett, Rockdale, Henry, Clayton, Fayette, Cobb, and Douglas
Honolulu, Hawaii	City of Honolulu; Honolulu County (Island of Oahu)
Chicago, Ill.	City of Chicago; Cook County, inclusive of 128 municipalities
Indianapolis, Ind.	City of Indianapolis; counties of Hamilton and Marion
Louisville, Ky.	City of Louisville; Louisville/Jefferson County Metro Government; inclusive of the cities of Jeffersontown, St. Matthews, Shively, and Anchorage. Secondary area inclusive of the Kentucky counties of Bullitt, Henry, Meade, Nelson, Oldham, Shelby, Spencer, and Trimble
Baton Rouge, La.	City of Baton Rouge; East Baton Rouge Parish; Louisiana Homeland Security Region 2 which includes East and West Baton Rouge Parish, East and West Feliciana Parish, Ascension Parish, Livingston Parish, Iberville Parish, and Pointe Coupee Parish
New Orleans, La.	City of New Orleans; Orleans Parish; parishes of Jefferson, St. Bernard, and Plaquemines.
Boston, Mass.	City of Boston; communities of Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Winthrop, and Somerville.
Baltimore, Md.	City of Baltimore; counties of Baltimore and Anne Arundel; City of Annapolis; counties of Carroll, Harford, and Howard.
Detroit, Mich.	City of Detroit; Wayne County
Minneapolis/St. Paul, Minn.	Cities of Minneapolis and St. Paul; counties of Hennepin, Ramsey, and Dakota.
Kansas City, Mo./Kan.	Cities of Kansas City (Mo.) and Kansas City (Kan.); counties of Cass, Clay, Jackson, Platte and Ray (Mo.); counties of Johnson, Leavenworth, and Wyandotte (Kan.)
St. Louis Mo./Ill.	City and County of St. Louis; counties of St. Charles, Franklin, and Jefferson (Mo.); counties of St. Clair, Madison, and Monroe (Ill.)
Omaha, Neb.	Douglas County
Charlotte, N.C.	City of Charlotte; Mecklenberg County; the counties of Union, Cabarrus, Stanly, Iredell, Catawba, Lincoln, and Gaston; supported by York and Lancaster in South Carolina
Jersey City/Newark, N.J. <sup>c</sup>	Cities of Jersey City and Newark; counties of Essex, Bergen, Hudson, Morris, Passaic, and Union
Las Vegas, Nev.	City of Las Vegas; Clark County
Buffalo, N.Y.	City of Buffalo; counties of Erie and Niagara

Table C.1—Continued

Urban Area	Defined Urban Area
New York, N.Y.	City of New York; counties of Nassau, Suffolk, and Westchester; Port Authority of New York and New Jersey
Cincinnati, Ohio	City of Cincinnati; Hamilton County, and the 49 local jurisdictions within the county
Cleveland, Ohio	City of Cleveland; County of Cuyahoga, inclusive of nine Cuyahoga Community Regions—Chagrin, Cleveland, Cuyahoga, Heights, Hillcrest, Southcentral, Southeast, Southwest, and Westshore, and the local jurisdictions therein
Columbus, Ohio	City of Columbus, Franklin County; the cities of Bexley, Columbus, Dublin, Grandview Heights, Grove City, Hilliard, Reynoldsburg, Upper Arlington, Westerville, Worthington, the villages of Brice, Canal Winchester, Groveport, Harrisburg, Lockbourne, Marble Cliff, Minerva Park, New Albany, Obetz, Urbancrest, Valleyview, the townships of Blendon, Brown, Clinton, Franklin, Hamilton, Jackson, Jefferson, Madison, Mifflin, Norwich, Perry, Plain, Pleasant, Prairie, Sharon, Truro, and Washington
Toledo, Ohio	Lucas County
Oklahoma City, Okla.	Oklahoma County, Canadian County, Cleveland County
Portland, Oreg.	City of Portland; counties of Washington, Multnomah, Clackamas, and Columbia (Oreg.); Clark County (Wash.)
Philadelphia, Pa.	City of Philadelphia; Philadelphia County; counties of Bucks, Chester, Delaware, and Montgomery
Pittsburgh, Pa.	City of Pittsburgh; counties of Allegheny, Armstrong, Beaver, Butler, Cambria, Fayette, Greene, Indiana, Lawrence, Mercer, Somerset, Washington, and Westmoreland
Dallas/Fort Worth area, Tex. <sup>d</sup>	City and County of Dallas; counties of Collin, Denton, Kaufman, and Rockwall; and the additional components of Tarrant County, DFW Airport, North Central Texas Council of Governments, and the DFW Hospital Council
Houston, Tex.	City of Houston; counties of Harris, Fort Bend, Montgomery, Brazoria, and Galveston; inclusive of Transit Authority and Port Authority
San Antonio, Tex.	City of San Antonio; the counties of Bexar and Comal; Alamo Area Councils of Government
Seattle, Wash.	City of Seattle; counties of King, Pierce, and Snohomish
Milwaukee, Wisc.	City of Milwaukee; counties of Milwaukee, Waukesha, and Washington

SOURCE: DHS Homeland Security Grant Program guidance kit (DHS, undated).

<sup>a</sup> The areas of Anaheim and Santa Ana, California, received separate UASI allocations but have been analyzed together as a single urban area.

<sup>b</sup> The areas of Los Angeles and Long Beach, California, received separate UASI allocations but have been analyzed together as a single urban area.

<sup>c</sup> The areas of Jersey City and Newark, New Jersey, received separate UASI allocations but have been analyzed together as a single urban area.

<sup>d</sup> The areas of Arlington, Dallas, and Fort Worth, Texas, received separate UASI allocations but have been analyzed together as a single urban area.





## Example of Filtering Risk-Analysis Results Using Intelligence Assessments of Terrorist Capabilities

---

Chapter Three describes how risk analysis could be used to focus both analysis and collection of intelligence. This process must address uncertainty about the required and actual capabilities of terrorist groups, intentions of terrorist groups, and consequences of different terrorism scenarios. This appendix provides an example of how this process might work by considering a subset of this problem: attack modes that terrorists might attempt. The RMS model was used to demonstrate the risk-analysis component of the approach.

We reviewed the NYPD case studies provided by OI&A to profile the resources available to terrorists in successful and unsuccessful terrorist attacks historically. These case studies were used because doing so allowed an opportunity for HITRAC to compare these results to those from other ongoing work.

The first step was to use the RMS model to estimate the resources required for different types of attack. Next, we examined three NYPD case studies: the 2000 attack on the USS *Cole* during refueling in Yemen's Aden Harbor, the Bali nightclub bombings that killed approximately 200 in 2004, and the investigations following the 1993 World Trade Center attack that revealed a conspiracy to target other New York City landmarks (referred to as the Landmark Plot). The NYPD case studies were used to assess terrorists' capabilities. Finally, we compared the capabilities of the terrorist groups that carried out or planned these attacks, as inferred from NYPD case studies, to the resource requirements in RMS for the attack modes used in each of these cases; that is, we filtered the RMS model scenarios using the NYPD scenario assessments as estimates of resources available for terrorist attacks. The set of terrorist attacks that pass this filter gives insight into what other attacks could be successfully executed by terrorists like those who planned the USS *Cole*, Bali nightclub, and Landmark Plot attacks.

### Assessing Required Capabilities for Terrorist Attacks

Table D.1 presents the logistics capabilities of the USS *Cole*, Bali, and Landmark Plot terrorists as implied by the NYPD investigations of these three case studies. For example, the terrorists in the USS *Cole* bombing were believed to have been trained in al Qaeda camps, six to eight people have been linked to the planning and implementation of this attack, the terrorists had access to at least \$500,000, and planning is believed to have taken place over at least 1.5 years.

**Table D.1**  
**Logistics Capabilities Implied by NYPD Case Studies**

Resource Requirement	USS <i>Cole</i> Attack, 2000	Bali Bombing, 2004	Landmark Plot, 1993
Skill level	Al Qaeda training	Not discussed	Paramilitary
Personnel	~6 to 8	~8	14
Capital	\$500k	> \$35k	Several \$k
Time	1.5 years	10 months	2 months

Similar analysis is presented for the Bali nightclub bombings and for the Landmark Plot of 1993. This analysis represents only our interpretation of information provided in the NYPD case studies and may not reflect all that is known about the events.

### Assessing Feasibility of Future Attacks

Capability assessments serve as input to help answer the question, What might terrorists with similar capabilities be able to do in the future? Given the assessments in Table D.1, we can next ask what types of attack would be possible by groups with these resources and skills. This question is answered by comparing intelligence estimates to the RMS model databases. First, we consider the terrorists who attacked the USS *Cole*.

The intelligence information contained in sources such as the NYPD scenarios can be compared to the attack mode resource requirements in the RMS model to filter out which attack mode–target pairs are inconsistent with presumed intelligence information. Applying this to the USS *Cole* bombing in 2000, analysis suggests that this terrorist group would have been capable of carrying out bomb attacks of 600 lb, 1 ton, and 2 tons; carrying out surface-to-air missile attacks; creating a conflagration by exploding a gasoline truck; or conducting industrial sabotage<sup>1</sup> on a small scale (see Table D.2). Other attack modes included in the RMS model would not have been possible given this assessment of the USS *Cole* terrorists' capabilities implied by the NYPD scenarios. It is worth noting that this figure does show that one of the listed attack modes would not have been possible given the assumed terrorist capabilities: a 5-ton bomb. The other 30 attack modes are likewise not shown because they too are inconsistent with the assumed terrorists' logistics capabilities.

Table D.2 presents a similar depiction of the capabilities of the Bali bombers, given the implied logistics capabilities from the NYPD scenarios and the information in the RMS model. Their limited capability stems from less planning time and money. As a result, largely based on the assumption of even more limited financial resources than the USS *Cole* terrorists possessed, the Bali bombing terrorists would presumably not have been capable of carrying out attacks using 1-, 2-, or 5-ton bombs. Once again, it is very important to note that these results

<sup>1</sup> In the RMS model, sabotage is modeled at oil refineries, chemical plants, and nuclear power plants that are in the model's target database.

**Table D.2**  
**Attack Modes That Terrorist Groups Involved in the USS *Cole* and Bali Bombing Terrorist Events Could Execute Based on Filtering of the RMS Model Using Assessments Made in NYPD Case Studies**

Attack Mode	Inferred Capabilities of USS <i>Cole</i> Terrorists	Inferred Capabilities of Bali Bombing Terrorists
Bomb: 600 lb.	x	x
Bomb: 1 ton	x	
Bomb: 2 ton	x	
Bomb: 5 ton		
Surface-to-air missile	x	x
Conflagration	x	x
Industrial sabotage: small	x	x

are dependent on assumptions in the RMS model, information in the NYPD scenarios, and our interpretation of the NYPD scenario documents.

The Landmark Plot of 1993 provides yet a different perspective on terrorists' capabilities. In this case study, the terrorists were caught before successfully attacking. On the basis of information in the NYPD scenario, the terrorists involved composed a larger group and had potentially greater knowledge and skill. However, they may have had less money available than those making the Bali or USS *Cole* attacks and appeared to have been planning over a much shorter period. As a result, analysis suggests that this group was not capable of any of the attack modes covered in the RMS model, given their fiscal and temporal resources. In this case, it is worth exploring how the results of the analysis would change with deviations from these assumptions. In particular, if they had received more money or had had more time, how would these conclusions change?

### Sensitivity Analysis Using Filtering Approach

We explore the sensitivity of this type of analysis for the 1993 Landmark Plot by considering how conclusions would change if estimates of terrorists' skills or resources changed. In the base case, NYPD scenarios suggested that planning began two months before the intended attack. If this group had three to six months instead, a rather small increase in the assumption about time, the analysis suggests that the group would have been capable of causing a conflagration or small industrial sabotage (see Table D.3). As it turns out, allowing even further time for planning does not change this result at all.

However, changing the financial resources available to the Landmark Plot terrorists does further change their capabilities. If the terrorists also had a modest increase in funding (-\$30,000) for capital expenditures, they could have also been capable of conducting an attack using a surface-to-air missile or a 600-lb bomb. This suggests that, without funding, the group

**Table D.3**  
**Sensitivity Analysis of Importance of Time and Financial Resources for Attack Mode Capabilities of 1993 Landmark Plot Terrorists**

Attack Mode	Capabilities of Landmark Plot, 1993	3–6 Months Versus 2 Months Planning	+ ~\$30k
Bomb: 600 lb.			x
Bomb: 1 ton			
Bomb: 2 ton			
Bomb: 5 ton			
SAM			x
Conflagration		x	x
Industrial sabotage: small		x	x

had the personnel and skill to carry out attacks, so long as they did not need to create their own explosive device, though with modest additional funding, they could have done so.

Extending this analysis further shows that continued increases in both funding and time allow such a group to be capable of larger sabotage attacks and larger bomb attacks. However, without significantly more skill, the group is still incapable of carrying out CBRN attacks successfully.

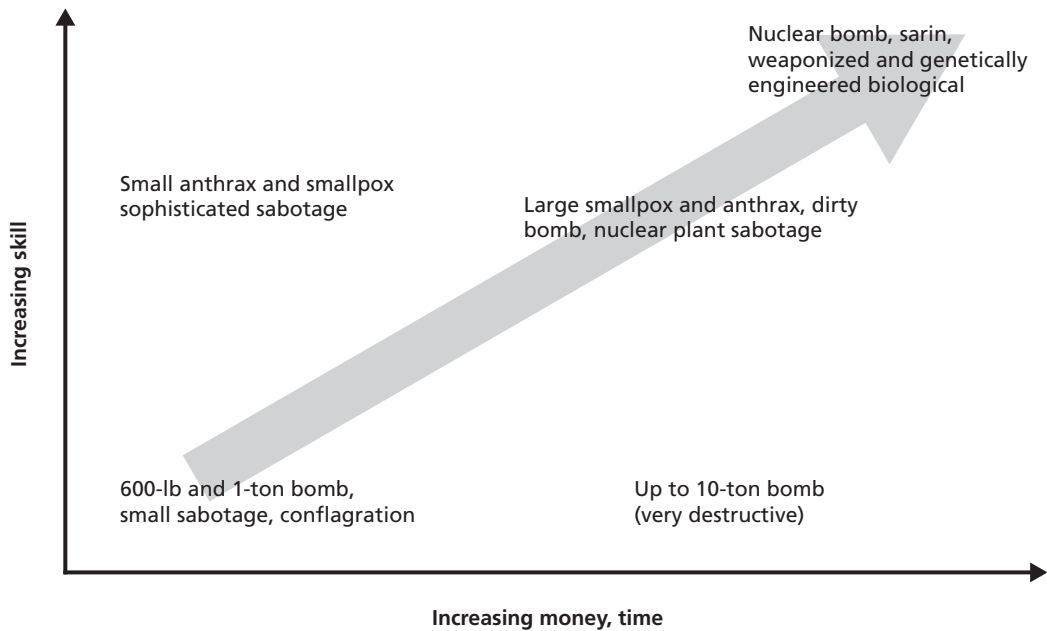
### The Relationship Between Logistics Burden and Attack Type

The results presented previously reveal several general observations about the assumed relationship between terrorist capabilities and possible attack modes. By exploring the dependence of different attack modes on the RMS model's estimates of individual component resources of the logistics burden, we find that increasing money and time can be generally distinguished from increasing skill in terms of their influence over attack mode options. This distinction is represented on a schematic showing skill on one axis and money and time on the other (Figure D.1). The capabilities determined for the terrorist groups profiled in the NYPD case studies limited these groups to the filtered set of attack modes shown in the lower left portion of the figure.

Increasing money and time without increasing skill allows terrorists to carry out more destructive attacks, but these are generally limited to larger bombs as the incremental logistics cost of increasing bomb size is primarily money and time rather than skill.

On the other hand, the RMS model suggests that, if money and time were limited but terrorists had access to greater skills, they could mount more technically complex attacks, such as more sophisticated sabotage and small biological attacks. Only with the combination of skill, money, and time can terrorists successfully mount most attacks involving CBRN weapons.

**Figure D.1**  
**Relationship Between Logistics Burden and Attack Type**



RAND TR386-D.1

## Extending Analysis to Provide Actionable Intelligence

This case study demonstrates how the RMS model could be used to suggest what attack modes or target types are feasible considering available intelligence information. However, how can we use this information to derive detailed intelligence guidance? Doing so requires knowledge of attack timelines and preparations. For example, what are the tasks that must be completed to acquire, assemble, and detonate a car bomb? What materials must be purchased? What type of surveillance is required? What types of support services are necessary? While this information is not contained in the RMS model, law enforcement and terrorism experts have documented many of these details. Connecting this information to the results discussed previously may help make this analytic tool more useful for the intelligence and law enforcement communities.

## Assumptions in This Analysis

Note that these results are dependent on assumptions in the RMS model, information in the NYPD scenarios, and our interpretation of the NYPD scenario documents. As noted previously, these were developed from literature and expert elicitation.

In addition, assessments of the capabilities required for terrorist attacks are based on RMS modeling assumptions. While these assumptions are clearly described and fully documented, they are nevertheless assumptions. If an intelligence agency has made independent assessments of these requirements, they could be included in this approach and compared to the RMS assessments.

To demonstrate the type of information the proposed approach would use and the type of results it would produce, the examples used the information in the NYPD case studies to describe capabilities of terrorists for past events. Source documents, other public information, and classified information could be easily integrated into this approach instead of the NYPD assessments.

The approach does not suggest what will or will not happen, but rather what attacks are likelier to occur. While a predictive model would be tremendously useful, it may not be possible to produce such a model at this point in our understanding of terrorism risk, and, in a world of limited resources and numerous possibilities, a tool that can help distinguish wheat from chaff can help direct resource allocations.

Finally, our work to date has been directed only at mining the information in the RMS model to demonstrate this tool. Further exercising of this approach will provide the best evaluation of its benefits. There are two significant challenges to the success of this approach. First, is the information required for translating intentions and capabilities into risk-analysis metrics obtainable? The limited case study presented here suggests that the answer to this question is yes. Second, can this type of analysis distinguish attack modes, targets, and terrorism scenarios with fine enough resolution to be useful for law enforcement? This case study does not provide a clear answer to this question. Its ultimate success may rest on what specific law enforcement functions are being supported and what specific risk-analysis tool is used.

## References

---

DHS—see U.S. Department of Homeland Security.

Dixon, Lloyd, John Arlington, Stephen J. Carroll, Darius N. Lakdawalla, Robert T. Reville, and David Adamson, *Issues and Options for Government Intervention in the Market for Terrorism Insurance*, Santa Monica, Calif.: RAND Corporation, OP-135-ICJ, 2004. As of August 30, 2007:  
[http://www.rand.org/pubs/occasional\\_papers/OP135/](http://www.rand.org/pubs/occasional_papers/OP135/)

Morgan, M. Granger, Max Henrion, and Mitchell Small, *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*, New York: Cambridge University Press, 1990.

RAND Center for Terrorism Risk Management Policy, undated homepage. As of August 30, 2007:  
<http://www.rand.org/multi/ctrmp/>

Risk Management Solutions, Probabilistic Terrorism Model, undated Web page. As of August 30, 2007:  
<http://www.rms.com/Terrorism/Solutions/ProbabilisticTerrorismModel.asp>

———, *RMS Terrorism Modeling: DHS National Planning Scenarios*, Newark, Calif., 2005.

RMS—see Risk Management Solutions.

U.S. Department of Homeland Security, *Fiscal Year 2005 Homeland Security Grant Program: Program Guidelines and Application Kit*, Washington, D.C., undated. As of August 30, 2007:  
<http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf>

———, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Washington, D.C., 2003. As of August 30, 2007:  
<http://purl.access.gpo.gov/GPO/LPS28728>

———, *National Infrastructure Protection Plan*, Washington, D.C., 2006. As of August 30, 2007:  
<http://purl.access.gpo.gov/GPO/LPS71533>

Willis, Henry H., Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby, *Estimating Terrorism Risk*, Santa Monica, Calif.: RAND Corporation, MG-388-RC, 2005. As of August 30, 2007:  
<http://www.rand.org/pubs/monographs/MG388/>