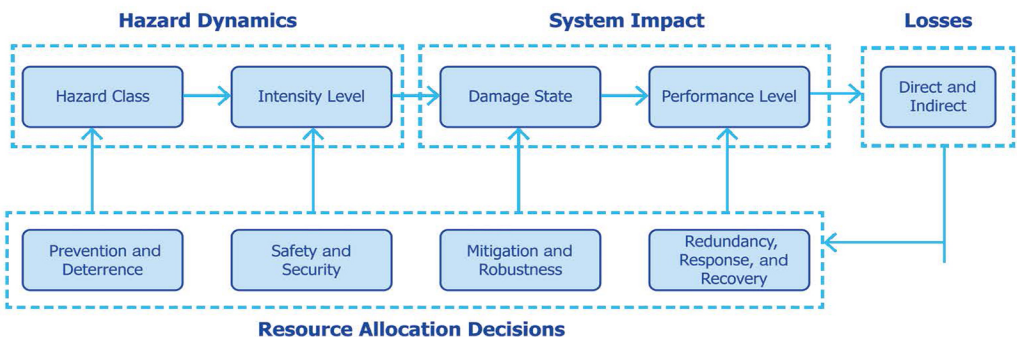


Wiley Series in Operations Research
and Management Science

EDITED BY

SAMRAT CHATTERJEE | ROBERT T. BRIGANTIC
ANGELA M. WATERWORTH

APPLIED RISK ANALYSIS FOR GUIDING HOMELAND SECURITY POLICY AND DECISIONS



WILEY

Applied Risk Analysis for Guiding Homeland Security Policy and Decisions

Wiley Series in

Operations Research and Management Science

Operations Research and Management Science (ORMS) is a broad, interdisciplinary branch of applied mathematics concerned with improving the quality of decisions and processes and is a major component of the global modern movement towards the use of advanced analytics in industry and scientific research. The *Wiley Series in Operations Research and Management Science* features a broad collection of books that meet the varied needs of researchers, practitioners, policy makers, and students who use or need to improve their use of analytics. Reflecting the wide range of current research within the ORMS community, the Series encompasses application, methodology, and theory and provides coverage of both classical and cutting edge ORMS concepts and developments. Written by recognized international experts in the field, this collection is appropriate for students as well as professionals from private and public sectors including industry, government, and nonprofit organization who are interested in ORMS at a technical level. The Series is comprised of four sections: Analytics; Decision and Risk Analysis; Optimization Models; and Stochastic Models.

Advisory Editors • Stochastic Models

Tava Olsen, The University of Auckland

Raúl Gouet, University of Chile

Founding Series Editor

James J. Cochran, University of Alabama

Analytics

Yang and Lee • *Healthcare Analytics: From Data to Knowledge to Healthcare Improvement*

Attoh-Okiné • *Big Data and Differential Privacy: Analysis Strategies for Railway Track Engineering*

Forthcoming Titles

Kong and Zhang • *Decision Analytics and Optimization in Disease Prevention and Treatment*

Behavioral Research

Donohue, Katok, and Leider • *The Handbook of Behavioral Operations*

Decision and Risk Analysis

Barron • *Game Theory: An Introduction*, Second Edition

Brailsford, Churilov, and Dangerfield • *Discrete-Event Simulation and System Dynamics for Management Decision Making*

Johnson, Keisler, Solak, Turcotte, Bayram, and Drew • *Decision Science for Housing and Community Development: Localized and Evidence-Based Responses to Distressed Housing and Blighted Communities*

Mislick and Nussbaum • *Cost Estimation: Methods and Tools*

Chatterjee, Brigantic, and Waterworth • *Applied Risk Analysis for Guiding Homeland Security Policy and Decisions*

Forthcoming Titles

Aleman and Carter • *Healthcare Engineering*

Optimization Models

Ghiani, Laporte, and Musmanno • *Introduction to Logistics Systems Management*, Second Edition

Forthcoming Titles

Tone • *Advances in DEA Theory and Applications: With Examples in Forecasting Models*

Stochastic Models

Ibe • *Random Walk and Diffusion Processes*

Forthcoming Titles

Matis • *Applied Markov Based Modelling of Random Processes*

Applied Risk Analysis for Guiding Homeland Security Policy and Decisions

Edited by

Samrat Chatterjee, Robert T. Brigantic, Angela M. Waterworth
Pacific Northwest National Laboratory, Richland, WA, USA

WILEY

This edition first published 2021

© 2021 John Wiley & Sons, Inc.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by law. Advice on how to obtain permission to reuse material from this title is available at <http://www.wiley.com/go/permissions>.

The right of Samrat Chatterjee, Robert T. Brigantic, Angela M. Waterworth to be identified as the editorial material in this work has been asserted in accordance with law.

Registered Office

John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

Editorial Office

111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Limit of Liability/Disclaimer of Warranty

While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials or promotional statements for this work. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Library of Congress Cataloging-in-Publication Data

Names: Chatterjee, Samrat, 1980- editor. | Brigantic, Robert T., editor. | Waterworth, Angela M., editor.

Title: Applied risk analysis for guiding homeland security policy and decisions / edited by Samrat Chatterjee, Robert T. Brigantic, Angela M. Waterworth.

Description: Hoboken, NJ : John Wiley & Sons, Inc., 2021. | Series: Wiley series in operations research and management science | Includes bibliographical references and index.

Identifiers: LCCN 2019057776 (print) | LCCN 2019057777 (ebook) | ISBN 9781119287469 (hardback) | ISBN 9781119287476 (adobe pdf) | ISBN 9781119287483 (epub)

Subjects: LCSH: United States. Department of Homeland Security--Management. | National security--United States. | Risk assessment--United States. | Risk management--United States. | Operations research--United States.

Classification: LCC UA23 .A684 2020 (print) | LCC UA23 (ebook) | DDC 363.34/5610973--dc23

LC record available at <https://lcn.loc.gov/2019057776>

LC ebook record available at <https://lcn.loc.gov/2019057777>

Cover Design: Wiley

Cover Image: Chart, courtesy of Samrat Chatterjee, abstract background © Toria /Shutterstock

Set in 10/12pt WarnockPro by SPi Global, Chennai, India

Samrat dedicates this book to his dearest Arianna, Aariv, Zyra, and Zara – stay curious, keep learning!

Robert dedicates this book to his lovely granddaughters Amelia Rose and Emmalyn Mae – blessings always!

Angela dedicates this book to Andy, Scarlett, and Archer

Contents

About the Editors	<i>xix</i>
List of Contributors	<i>xxi</i>
Preface	<i>xxv</i>
Chapter Abstracts	<i>xxviii</i>

Part I Managing National Security Risk and Policy Programs 1

1	On the “Influence of Scenarios to Priorities” in Risk and Security Programs 3
	<i>Heimir Thorisson and James H. Lambert</i>
1.1	Introduction 3
1.2	Risk Programs 4
1.3	Canonical Questions Guiding Development of Risk Programs 6
1.3.1	Canonical Question I: Scope 6
1.3.2	Canonical Question II: Operational Design 7
1.3.3	Canonical Question III: Evaluation 7
1.4	Scenario-Based Preferences 8
1.5	Methodology 9
1.6	Demonstration of Methods 12
1.7	Discussion and Conclusions 20
	Acknowledgments 22
	References 22
2	Survey of Risk Analytic Guidelines Across the Government 25
	<i>Isaac Maya, Amelia Liu, Lily Zhu, Francine Tran, Robert Creighton and Charles Woo</i>
2.1	Department of Defense (DOD) Overview 25
2.1.1	Joint Risk Analysis Methodology (JRAM) for the Chairman’s Risk Assessment (CRA) 26

2.1.2	Mission Assurance (MA): Risk Assessment and Management for DOD Missions	29
2.1.3	Risk Management Guide for DOD Acquisition	31
2.2	Department of Justice (DOJ)	33
2.3	Environmental Protection Agency (EPA) Overview	36
2.3.1	EPA Risk Leadership	36
2.3.2	EPA Risk Assessment Methodology and Guidelines	37
2.3.3	Risk Assessment Case Studies	40
2.3.4	Risk Assessment Challenges of EPA	43
2.3.5	Review of EPA Risk Assessment/Risk Management Methodologies	43
2.4	National Aeronautics and Space Administration (NASA): Overview	44
2.4.1	NASA Risk Leadership	44
2.4.2	Critical Steps in NASA Risk Assessment/Risk Management	44
2.4.3	Risk Assessment/Risk Management Challenges of NASA	48
2.4.4	Review of NASA Risk Assessment/Risk Management Methodologies	49
2.5	Nuclear Regulatory Commission (NRC) Overview	49
2.5.1	NRC Leadership	51
2.5.2	Critical Steps in NRC Risk Assessment/Risk Management	52
2.5.3	Risk Assessment/Risk Management Challenges of NRC	53
2.5.4	Review of NRC Risk Assessment/Risk Management Methodologies	54
2.6	International Standards Organization (ISO) Overview	55
2.6.1	ISO Leadership	57
2.6.2	Critical Steps in ISO Risk Assessment/Risk Management	57
2.6.3	Risk Assessment/Risk Management Challenges of ISO	58
2.7	Australia Overview	58
2.7.1	Australia Leadership	59
2.7.2	Critical Steps in Australia Risk Assessment/Risk Management	60
2.7.3	Risk Assessment/Risk Management Challenges of Australia	61
2.8	UK Overview	61
2.8.1	UK Leadership	61
2.8.2	Critical Steps in UK Risk Assessment/Risk Management	62
2.8.3	Risk Assessment/Risk Management Challenges of the United Kingdom	65
	Acknowledgments	65
	References	65

3	An Overview of Risk Modeling Methods and Approaches for National Security	69
	<i>Samrat Chatterjee, Robert T. Brigantic and Angela M. Waterworth</i>	
3.1	Introduction	69
3.2	Homeland Security Risk Landscape and Missions	70
3.2.1	Risk Landscape	71
3.2.2	Security Missions	71
3.2.3	Risk Definitions and Interpretations from DHS Risk Lexicon	72
3.3	Background Review	73
3.3.1	1960s to 1990s: Focus on Foundational Concepts	73
3.3.2	The 2000s: Increased Focus on Multi-hazard Risks Including Terrorism	75
3.3.3	2009 to Present: Emerging Emphasis on System Resilience and Complexity	78
3.4	Modeling Approaches for Risk Elements	88
3.4.1	Threat Modeling	88
3.4.2	Vulnerability Modeling	88
3.4.2.1	Survey-Based Methods	88
3.4.2.2	Systems Analysis	89
3.4.2.3	Network-Theoretic Approaches	89
3.4.2.4	Structural Analysis and Reliability Theory	89
3.4.3	Consequence Modeling	89
3.4.3.1	Direct Impacts	89
3.4.3.2	Indirect Impacts	89
3.4.4	Risk-Informed Decision Making	90
3.5	Modeling Perspectives for Further Research	90
3.5.1	Systemic Risk and Resilience Within a Unified Framework	90
3.5.2	Characterizing Cyber and Physical Infrastructure System Behaviors and Hazards	91
3.5.3	Utilizing “Big” Data or Lack of Data for Generating Risk and Resilience Analytics	91
3.5.4	Conceptual Multi-scale, Multi-hazard Modeling Framework	92
3.6	Concluding Remarks	94
	Acknowledgments	95
	References	95
4	Comparative Risk Rankings in Support of Homeland Security Strategic Plans	101
	<i>Russell Lundberg</i>	
4.1	Introduction	101
4.2	Conceptual Challenges in Comparative Risk Ranking	102

4.3	Practical Challenges in Comparative Ranking of Homeland Security Risks	103
4.3.1	Choosing a Risk Set	104
4.3.1.1	Lessons from the DMRR on Hazard Set Selection	105
4.3.2	Identifying Attributes to Consider	105
4.3.2.1	Lessons from the DMRR on Attribute Selection	107
4.3.3	Assessing Each Risk Individually	109
4.3.3.1	Lessons from the DMRR on Assessing Individual Homeland Security Risks	111
4.3.4	Combining Individual Risks to Develop a Comparative Risk Ranking	112
4.3.4.1	Lessons from the DMRR on Comparing Homeland Security Risks	114
4.4	Policy Relevance to Strategic-Level Homeland Security Risk Rankings	116
4.4.1	Insights into Homeland Security Risk Rankings	116
4.4.2	Risk vs. Risk Reduction	118
	Acknowledgments	120
	References	120
5	A Data Science Workflow for Discovering Spatial Patterns Among Terrorist Attacks and Infrastructure	125
	<i>Daniel C. Fortin, Thomas Johansen, Samrat Chatterjee, George Muller and Christine Noonan</i>	
5.1	Introduction	125
5.2	The Data: Global Terrorism Database	126
5.3	The Tools: Exploring Data Interactively Using a Custom Shiny App	127
5.4	Example: Using the App to Explore ISIL Attacks	130
5.5	The Models: Statistical Models for Terrorist Event Data	134
5.6	More Data: Obtaining Regional Infrastructure Data to Build Statistical Models	135
5.7	A Model: Determining the Significance of Infrastructure on the Likelihood of an Attack	137
5.8	Case Study: Libya	138
5.9	Case Study: Jammu and Kashmir Region of India	139
5.9.1	The Model Revisited: Accounting for Many Regions with No Recorded Attacks	141
5.9.2	Investigating the Effect of Outliers	145
5.9.3	The Insight: What Have We Learned?	147
5.10	Summary	148
	References	148

Part II Strengthening Ports of Entry 151

- 6 Effects of Credibility of Retaliation Threats in Deterring Smuggling of Nuclear Weapons 153**
Xiaojun Shan and Jun Zhuang
 - 6.1 Introduction 153
 - 6.2 Extending Prior Game-Based Model 158
 - 6.3 Comparing the Game Trees 158
 - 6.4 The Extended Model 161
 - 6.5 Solution to the Extended Model 162
 - 6.6 Comparing the Solutions in Prior Game-Based Model and This Study 163
 - 6.7 Illustration of the Extended Model Using Real Data 164
 - 6.8 Conclusion and Future Research Work 165
References 167
- 7 Disutility of Mass Relocation After a Severe Nuclear Accident 171**
Vicki M. Bier and Shuji Liu
 - 7.1 Introduction 171
 - 7.2 Raw Data 174
 - 7.3 Trade-Offs Between Cancer Fatalities and Relocation 177
 - 7.4 Risk-Neutral Disutility Model 179
 - 7.5 Risk-Averse Disutility Model 179
 - 7.6 Disutility Model with Interaction Effects 182
 - 7.7 Economic Analysis 185
 - 7.8 Conclusion 190
References 191
- 8 Scheduling Federal Air Marshals Under Uncertainty 193**
Keith W. DeGregory and Rajesh Ganesan
 - 8.1 Introduction 193
 - 8.2 Literature 196
 - 8.2.1 Commercial Aviation Industry 196
 - 8.2.2 Homeland Security and the Federal Air Marshals Service 198
 - 8.2.3 Approximate Dynamic Programming 199
 - 8.3 Air Marshal Resource Allocation Model 200
 - 8.3.1 Risk Model 200
 - 8.3.2 Static Allocation 202
 - 8.3.3 Dynamic Allocation 203
 - 8.4 Stochastic Dynamic Programming Formulation 204
 - 8.4.1 System State 205

8.4.2	Decision Variable	205
8.4.3	Post-decision State	206
8.4.4	Exogenous Information	206
8.4.5	State Transition Function	206
8.4.6	Contribution Function	206
8.4.7	Objective Function	207
8.4.8	Bellman's Optimality Equations	207
8.5	Phases of Stochastic Dynamic Programming	207
8.5.1	Exploration Phase	207
8.5.2	Learning Phase	208
8.5.2.1	Algorithm	208
8.5.2.2	Approximation Methods	208
8.5.2.3	Convergence	209
8.5.3	Learned Phase	210
8.6	Integrated Allocation Model	210
8.7	Results	211
8.7.1	Experiment	211
8.7.2	Results from Stochastic Dynamic Programming Model	211
8.7.3	Sensitivity Analysis	212
8.7.4	Model Output	214
8.8	Conclusion	217
	Acknowledgments	218
	References	218

Part III Securing Critical Cyber Assets 221

9	Decision Theory for Network Security: Active Sensing for Detection and Prevention of Data Exfiltration	223
	<i>Sara M. McCarthy, Arunesh Sinha, Milind Tambe and Pratyusa Manadhatha</i>	
9.1	Introduction	223
9.1.1	Problem Domain	224
9.2	Background and Related Work	226
9.2.1	DNS Exfiltration	226
9.2.2	Partially Observable Markov Decision Process (POMDP)	228
9.3	Threat Model	229
9.3.1	The POMDP Model	230
9.4	POMDP Abstraction	232
9.4.1	Abstract Actions	232
9.4.2	Abstract Observations	234
9.4.3	VD-POMDP Factored Representation	234
9.4.4	Policy Execution	236
9.5	VD-POMDP Framework	239
9.6	Evaluation	241

9.6.1	Synthetic Networks	241
9.6.2	DETER Testbed Simulation	241
9.6.3	Runtime	242
9.6.4	Performance	244
9.6.5	Robustness	246
9.7	Game Theoretic Extensions	247
9.7.1	Threat Model	248
9.8	Conclusion and Future Work	249
	Acknowledgments	249
	References	249
10	Measurement of Cyber Resilience from an Economic Perspective	253
	<i>Adam Z. Rose and Noah Miller</i>	
10.1	Introduction	253
10.2	Economic Resilience	254
10.2.1	Basic Concepts of Cyber Resilience	254
10.2.2	Basic Concepts of Economic Resilience	254
10.2.3	Economic Resilience Metrics	255
10.3	Cyber System Resilience Tactics	257
10.4	Resilience for Cyber-Related Sectors	267
10.4.1	Resilience in the Manufacturing of Cyber Equipment	267
10.4.2	Resilience in the Electricity Sector	268
10.5	Conclusion	269
	References	270
11	Responses to Cyber Near-Misses: A Scale to Measure Individual Differences	275
	<i>Jinshu Cui, Heather Rosoff and Richard S. John</i>	
11.1	Introduction	275
11.2	Scale Development and Analysis Outline	277
11.3	Method	278
11.3.1	Measures	278
11.3.1.1	Cyber Near-Miss Appraisal Scale (CNMAS)	278
11.3.1.2	Measures of Discriminant Validity	281
11.3.1.3	Measure of Predictive Validity	281
11.3.1.4	Participants and Procedures	281
11.4	Results	284
11.4.1	Dimensionality and Reliability	284
11.4.2	Item Response Analysis	284
11.4.3	Differential Item Functioning (DIF)	287
11.4.4	Effects of Demographic Variables	289
11.4.5	Discriminant Validity	290
11.4.6	Predictive Validity	290

11.5	Discussion	291
	Acknowledgments	292
	References	292

Part IV Enhancing Disaster Preparedness and Infrastructure Resilience 295

12	An Interactive Web-Based Decision Support System for Mass Dispensing, Emergency Preparedness, and Biosurveillance	297
	<i>Eva K. Lee, Ferdinand H. Pietz, Chien-Hung Chen and Yifan Liu</i>	
12.1	Introduction	297
12.2	System Architecture and Design	299
12.3	System Modules and Functionalities	301
12.3.1	Interactive User Experience	301
12.3.2	Geographical Boundaries	301
12.3.3	Network of Service, Locations, and Population Flow and Assignment	302
12.3.4	ZIP Code and Population Composition	304
12.3.5	Multimodality Dispensing and Public–Private Partnership	305
12.3.6	POD Layout Design and Resource Allocation	308
12.3.7	Radiological Module	309
12.3.8	Biosurveillance	309
12.3.9	Regional Information Sharing, Reverse Reporting, Tracking and Monitoring, and Resupply	310
12.3.10	Multilevel End-User Access	311
12.4	Biodefense, Pandemic Preparedness Planning, and Radiological and Large-Scale Disaster Relief Efforts	312
12.4.1	Biodefense Mass Dispensing Regional Planning	312
12.4.2	Real-Life Disaster Response Effort	315
12.4.2.1	RealOpt-Haiti©	315
12.4.2.2	RealOpt-Regional and RealOpt-CRC for Fukushima Daiichi Nuclear Disaster	316
12.4.2.3	RealOpt-ASSURE©	318
12.5	Challenges and Conclusions	319
	Acknowledgments	321
	References	321
13	Measuring Critical Infrastructure Risk, Protection, and Resilience in an All-Hazards Environment	325
	<i>Julia A. Phillips and Frédéric Petit</i>	
13.1	Introduction to Critical Infrastructure Risk Assessment	325
13.2	Motivation for Critical Infrastructure Risk Assessments	326

13.2.1	Unrest pre-September 2001	326
13.2.2	Post-911 Critical Infrastructure Protection and Resilience	326
13.3	Decision Analysis Methodologies for Creating Critical Infrastructure Risk Indicators	327
13.3.1	Decision Analysis	328
13.3.2	Illustrative Calculations for an Index: Buying a Car	328
13.4	An Application of Critical Infrastructure Protection, Consequence, and Resilience Assessment	331
13.4.1	Protection and Vulnerability	334
13.4.1.1	Physical Security	335
13.4.1.2	Security Management	335
13.4.1.3	Security Force	335
13.4.1.4	Information Sharing	337
13.4.1.5	Security Activity Background	338
13.4.2	Resilience	339
13.4.2.1	Preparedness	341
13.4.2.2	Mitigation Measures	341
13.4.2.3	Response Capabilities	342
13.4.2.4	Recovery Mechanisms	343
13.4.3	Consequences	343
13.4.3.1	Human Consequences	345
13.4.3.2	Economic Consequences	346
13.4.3.3	Government Mission/Public Health/Psychological Consequences	346
13.4.3.4	Cascading Impact Consequences	347
13.4.4	Risk Indices Comparison	349
13.5	Infrastructure Interdependencies	350
13.6	What's Next for Critical Infrastructure Risk Assessments	352
	References	354
14	Risk Analysis Methods in Resilience Modeling: An Overview of Critical Infrastructure Applications	357
	<i>Hiba Baroud</i>	
14.1	Introduction	357
14.2	Background	358
14.2.1	Risk Analysis	358
14.2.2	Resilience	359
14.2.3	Critical Infrastructure Systems	360
14.3	Modeling the Resilience of Critical Infrastructure Systems	361
14.3.1	Resilience Models	361
14.3.1.1	Manufacturing	361
14.3.1.2	Communications	362
14.3.1.3	Dams, Levees, and Waterways	363
14.3.1.4	Defense	363

14.3.1.5	Emergency Services	363
14.3.1.6	Energy	363
14.3.1.7	Transportation	364
14.3.1.8	Water/Wastewater	364
14.3.2	Discussion	365
14.3.2.1	Economic Impact	365
14.3.2.2	Social Impact	367
14.3.2.3	Interdependencies	367
14.4	Assessing Risk in Resilience Models	368
14.4.1	Probabilistic Methods	368
14.4.2	Uncertainty Modeling	369
14.4.3	Simulation-Based Approaches	369
14.4.4	Data-Driven Analytics	370
14.5	Opportunities and Challenges	370
14.5.1	Opportunities	370
14.5.2	Challenges	371
14.6	Concluding Remarks	372
	References	373
15	Optimal Resource Allocation Model to Prevent, Prepare, and Respond to Multiple Disruptions, with Application to the <i>Deepwater Horizon</i> Oil Spill and Hurricane Katrina	381
	<i>Cameron A. MacKenzie and Amro Al Kazimi</i>	
15.1	Introduction	381
15.2	Model Development	383
15.2.1	Resource Allocation Model	383
15.2.2	Extension to Uncertain Parameters	385
15.3	Application: <i>Deepwater Horizon</i> and Hurricane Katrina	386
15.3.1	Parameter Estimation	386
15.3.1.1	Oil Spill Parameters	387
15.3.1.2	Hurricane Parameters	388
15.3.2	Base Case Results	391
15.3.3	Sensitivity Analysis on Economic Impacts	394
15.3.4	Model with Uncertain Effectiveness	395
15.4	Conclusions	397
	References	398
16	Inoperability Input–Output Modeling of Electric Power Disruptions	405
	<i>Joost R. Santos, Sheree Ann Pagsuyoin and Christian Yip</i>	
16.1	Introduction	405
16.2	Risk Analysis of Natural and Man-Caused Electric Power Disruptions	407

16.3	Risk Management Insights for Disruptive Events	408
16.4	Modeling the Ripple Effects for Disruptive Events	411
16.5	Inoperability Input–Output Model	412
16.5.1	Model Parameters	412
16.5.2	Sector Inoperability	413
16.5.3	Interdependency Matrix	413
16.5.4	Demand Perturbation	414
16.5.5	Economic Resilience	414
16.5.6	Economic Loss	415
16.6	Sample Electric Power Disruptions Scenario Analysis for the United States	416
16.7	Summary and Conclusions	421
	References	422
17	Quantitative Assessment of Transportation Network Vulnerability with Dynamic Traffic Simulation Methods	427
	<i>Venkateswaran Shekar and Lance Fiondella</i>	
17.1	Introduction	427
17.2	Dynamic Transportation Network Vulnerability Assessment	429
17.3	Sources of Input for Dynamic Transportation Network Vulnerability Assessment	431
17.4	Illustrations	432
17.4.1	Example 1: Simple Network	432
17.4.2	Example II: University of Massachusetts Dartmouth Evacuation	437
17.5	Conclusion and Future Research	439
	References	440
18	Infrastructure Monitoring for Health and Security	443
	<i>Prodyot K. Basu</i>	
18.1	Introduction	443
18.2	Data Acquisition	447
18.3	Sensors	447
18.3.1	Underlying Principles of Some of the Popular Sensors Listed in Table 18.1	451
18.3.1.1	Fiber Optics	451
18.3.1.2	Vibrating Wire	451
18.3.1.3	Piezoelectric Sensors	456
18.3.1.4	Piezoresistive Sensors	456
18.3.1.5	Laser Vibrometer	456
18.3.1.6	Acoustic Emission Sensing	457
18.3.1.7	GPS and GNSS	458
18.3.2	Selection of a Sensor	459

18.4	Capturing and Transmitting Signals	459
18.5	Energy Harvesting	461
18.6	Robotic IHM	462
18.7	Cyber-Physical Systems	464
18.8	Conclusions	464
	References	465
19	Exploring Metaheuristic Approaches for Solving the Traveling Salesman Problem Applied to Emergency Planning and Response	467
	<i>Ramakrishna Tipireddy, Javier Rubio-Herrero, Samrat Chatterjee and Satish Chikkagoudar</i>	
19.1	The Traveling Salesman Problem	467
19.1.1	Definition	467
19.1.2	Computational Complexity	467
19.1.3	Solution Algorithms	468
19.1.4	Emergency Response Application	468
19.2	Emergency Planning and Response as a Traveling Salesman Problem	468
19.3	Metaheuristic Approaches	469
19.3.1	Simulated Annealing	470
19.3.1.1	Overview	470
19.3.1.2	Pseudocode	471
19.3.1.3	Case Study Results	473
19.3.2	Tabu Search	473
19.3.2.1	Overview	473
19.3.2.2	Pseudocode	474
19.3.2.3	Case Study Results	476
19.3.3	Genetic Algorithms	476
19.3.3.1	Overview	476
19.3.3.2	Pseudocode	478
19.3.3.3	Case Study Results	479
19.3.4	Ant Colony Optimization	479
19.3.4.1	Overview	479
19.3.4.2	Stochastic Solution Construction	480
19.3.4.3	Pheromone Update	480
19.3.4.4	Pseudocode	481
19.3.4.5	Case Study Results	481
19.4	Discussion	482
19.5	Concluding Remarks	482
	References	484

About the Editors

Dr. Samrat Chatterjee is a Senior Data/Operations Research Scientist and the Decision Modeling and Optimization Team Lead with the National Security Directorate at the Pacific Northwest National Laboratory (PNNL). His research focuses on assessing and managing risks to critical cyber and physical infrastructure systems and processes from multiple hazards using interdisciplinary modeling, simulation, data analytics, and operations research methods. His research activities at PNNL focus on national security in support of the Department of Homeland Security, Department of Energy, and the Department of Defense. He recently co-authored a Springer book on economic consequence analysis of disasters and has published over 65 peer-reviewed journal articles, conference papers, and technical reports, including two best paper awards in cybersecurity and disaster resilience at an Institute of Electrical and Electronics Engineers (IEEE) homeland security conference. He is current chair of the Security and Defense specialty group, and past chair of the Engineering and Infrastructure specialty group of the Society for Risk Analysis (SRA), and recently completed a membership term with the National Academies' Transportation Research Board's (TRB) Committee on Transportation of Hazardous Materials. His experience includes disaster risk modeling at the International Institute for Applied Systems Analysis (IIASA) in Austria on a National Academy of Sciences (NAS) fellowship through a National Science Foundation (NSF) grant and traffic flow simulation for an engineering consulting firm. Samrat conducted postdoctoral research on infrastructure risk and decision analysis at the US Homeland Security National Center of Excellence for Risk and Economic Analysis of Terrorism Events (DHS-CREATE) at the University of Southern California. Dr. Chatterjee holds a PhD in Civil Engineering with focus on systems risk analysis from Vanderbilt University, an MS in Civil Engineering with focus on transportation systems from the University of Texas at Austin, and a BE with honors in Civil Engineering from Punjab Engineering College, India. Samrat also serves as an Affiliate Professor of Civil and Environmental Engineering with Northeastern

University in Boston. He is a senior member of IEEE, and member of SRA and the Military Operations Research Society (MORS).

Dr. Robert T. Brigantic is a Chief Operations Research Scientist and the Statistical Modeling and Experimental Design Team Lead with the National Security Directorate at the Pacific Northwest National Laboratory (PNNL). He is a US Air Force officer who joined PNNL in 2005 after completing a 22-year career on active duty with the US Air Force. In the Air Force he specialized in weapon systems logistics, space operations with a focus on command and control systems for space shuttle operations and space test systems, and strategic airlift transportation. His technical concentration areas include operational modeling and simulation, systems analysis, statistical pattern recognition/artificial intelligence, imagery analysis, design of experiments, and multiobjective optimization. At PNNL, some of his research initiatives include operationalizing methodologies for national security risk analysis, modeling and simulation of operational radiation/nuclear detection processes, systems analysis, and optimization of renewable energy systems and energy efficiency measures. Dr. Brigantic holds a PhD in Operations Research from the Air Force Institute of Technology, an MS in Space Operations from the Air Force Institute of Technology, and a BS in Chemical Engineering from Oregon State University. He also serves as an Adjunct Professor of Operations Research with Washington State University.

Ms. Angela M. Waterworth is a Senior Research Scientist with the National Security Directorate at the Pacific Northwest National Laboratory (PNNL) and currently serves as the Technical Advisor for Data Science for Defense Nuclear Nonproliferation Research and Development at the National Nuclear Security Administration. Ms. Waterworth joined PNNL after a distinguished career as an Operations Research Analyst in the US Air Force, where she specialized in research and development and technical intelligence of weapon systems. At PNNL, Ms. Waterworth has led project teams to develop operational modeling and decision support methodologies to analyze and reduce system risk, forecast cost and performance, and optimize resource allocation related to real-world national security systems for threats including nuclear proliferation and smuggling and emergency response to biological weapons. Additionally, Ms. Waterworth leads multidisciplinary efforts in the research and development of US technical capabilities to detect nuclear weapons development, with special focus on incorporating modern analytics approaches and computing technologies. Ms. Waterworth holds an MS in Operations Research from Kansas State University and a BS in Economics from the US Air Force Academy.

List of Contributors

Amro Al- Kazimi

Industrial and Manufacturing
Systems Engineering
Iowa State University
Ames, IA, USA

Hiba Baroud

Civil and Environmental Engineering
Vanderbilt University
Nashville, TN, USA

Prodyot K. Basu

Civil and Environmental Engineering
Vanderbilt University
Nashville, TN, USA

Vicki M. Bier

Industrial and Systems Engineering
University of Wisconsin–Madison
Madison, WI, USA

Robert T. Brigantic

National Security Directorate
Pacific Northwest National
Laboratory
Richland, WA, USA

Samrat Chatterjee

National Security Directorate
Pacific Northwest National
Laboratory
Richland, WA, USA

Satish Chikkagoudar

National Security Directorate
Pacific Northwest National
Laboratory
Richland, WA, USA

Chien-Hung Chen

Industrial and Systems Engineering
Georgia Institute of Technology
Atlanta, GA, USA

Robert Creighton

National Center for Risk and
Economic Analysis of Terrorism
Events (CREATE)
University of Southern California
Los Angeles, CA, USA

Jinshu Cui

Department of Psychology
University of Southern California
Los Angeles, CA, USA

Keith W. DeGregory

United States Military Academy
West Point, NY, USA

Daniel C. Fortin

National Security Directorate
Pacific Northwest National
Laboratory
Richland, WA, USA

Lance Fiondella

Electrical and Computer Engineering
University of Massachusetts
Dartmouth
Dartmouth, MA, USA

Rajesh Ganesan

Systems Engineering and Operations
Research
George Mason University
Fairfax, VA, USA

Thomas Johansen

National Security Directorate
Pacific Northwest National
Laboratory
Richland, WA, USA

Richard S. John

Department of Psychology
University of Southern California
Los Angeles, CA, USA

James H. Lambert

Systems and Information
Engineering
University of Virginia
Charlottesville, VA, USA

Eva K. Lee

Industrial and Systems Engineering
Georgia Institute of Technology
Atlanta, GA, USA

Amelia Liu

National Center for Risk and
Economic Analysis of Terrorism
Events (CREATE)
University of Southern California
Los Angeles, CA, USA

Shuji Liu

Industrial and Systems Engineering
University of Wisconsin–Madison
Madison, WI, USA

Yifan Liu

Industrial and Systems Engineering
Georgia Institute of Technology
Atlanta, GA, USA

Russell Lundberg

College of Criminal Justice
Sam Houston State University
Huntsville, TX, USA

Cameron A. MacKenzie

Industrial and Manufacturing
Systems Engineering
Iowa State University
Ames, IA, USA

Pratyusa Manadhatha

Hewlett Packard Labs
Princeton, NJ, USA

Isaac Maya

National Center for Risk and
Economic Analysis of Terrorism
Events (CREATE)
University of Southern California
Los Angeles, CA, USA

Sara M. McCarthy

Department of Computer Science
University of Southern California
Los Angeles, CA, USA

Noah Miller

National Center for Risk and
Economic Analysis of Terrorism
Events (CREATE)
University of Southern California
Los Angeles, CA, USA

George Muller

National Security Directorate
Pacific Northwest National
Laboratory
Richland, WA, USA

Christine Noonan

National Security Directorate
Pacific Northwest National
Laboratory
Richland, WA, USA

Sheree Ann Pagsuyoin

Civil and Environmental Engineering
University of Massachusetts–Lowell
Lowell, MA, USA

Frédéric Petit

Risk and Infrastructure Science
Center
Argonne National Laboratory
Argonne, IL, USA

Julia A. Phillips

The Perduco Group
Dayton, OH, USA

Ferdinand H. Pietz

Centers for Disease Control and
Prevention
Atlanta, GA, USA

Adam Z. Rose

National Center for Risk and
Economic Analysis of Terrorism
Events (CREATE)
University of Southern California
Los Angeles, CA, USA

Heather Rosoff

National Center for Risk and
Economic Analysis of Terrorism
Events (CREATE)
University of Southern California
Los Angeles, CA, USA

Javier Rubio-Herrero

School of Science, Engineering, and
Technology
St. Mary's University
San Antonio, TX, USA

Joost R. Santos

Engineering Management and
Systems Engineering
George Washington University
Washington, DC, USA

Xiaojun Shan

Industrial and Systems Engineering
State University of New York at
Buffalo
Buffalo, NY, USA

Venkateswaran Shekar

Electrical and Computer Engineering
University of Massachusetts
Dartmouth
Dartmouth, MA, USA

Arunesh Sinha

Department of Computer Science
University of Southern California
Los Angeles, CA, USA

Milind Tambe

Department of Computer Science &
Industrial and Systems Engineering
University of Southern California
Los Angeles, CA, USA

Heimir Thorisson

Systems and Information
Engineering
University of Virginia
Charlottesville, VA, USA

Ramakrishna Tipireddy

Physical and Computational Sciences
Directorate
Pacific Northwest National
Laboratory
Richland, WA, USA

Francine Tran

National Center for Risk and
Economic Analysis of Terrorism
Events (CREATE)
University of Southern California
Los Angeles, CA, USA

Angela M. Waterworth

National Security Directorate
Pacific Northwest National
Laboratory
Richland, WA, USA

Charles Woo

National Center for Risk and
Economic Analysis of Terrorism
Events (CREATE)
University of Southern California
Los Angeles, CA, USA

Christian Yip

Engineering Management and
Systems Engineering
George Washington University
Washington, DC, USA

Lily Zhu

National Center for Risk and
Economic Analysis of Terrorism
Events (CREATE)
University of Southern California
Los Angeles, CA, USA

Jun Zhuang

Industrial and Systems Engineering
State University of New York at
Buffalo
Buffalo, NY, USA

Preface

The US Department of Homeland Security's (DHS) risk landscape spans across multiple intentional, accidental, and natural threats and hazards. These threats and hazards may be directed at and affect various critical national assets, systems, and processes and potentially lead to significant adverse human, societal, economic, and governance impacts. As a result, effective assessment and management of risks to the nation's security from such threats and hazards is both vital and challenging. As described in the 2014 Quadrennial Homeland Security Review (Department of Homeland Security (2014) *The 2014 Quadrennial Homeland Security Review*), DHS's five missions are to: (i) prevent terrorism and enhance security, (ii) secure and manage our borders, (iii) enforce and administer our immigration laws, (iv) safeguard and secure cyberspace, and (v) strengthen national preparedness and resilience. Analysis and comparison of risks from various threats and hazards is critical for accomplishing these missions. Also, as these threats and hazards evolve over time and critical systems become more connected and complex, risk assessment and management strategies need to adequately update as well while incorporating data and computing advances with subject matter expertise.

Risk analysis methods may be qualitative, semiquantitative, or quantitative, adopt probabilistic and statistical theories, and implement concepts from core disciplines including operations research, reliability engineering, systems engineering, and applied mathematics. These methods continue to develop and evolve and have successfully been applied to address various homeland security mission challenges in recent years. The objective of this edited volume is to: (i) highlight the role of risk science for informing homeland security policy decisions and (ii) describe case studies from academia, government, and industry that apply risk analysis methods for addressing challenges within DHS mission spaces. This volume is intended for homeland security policy analysts and practitioners interested in applications of security risk analysis methods. The content presented here might also be useful for researchers and students interested in state-of-the-art homeland security risk analysis research and development.

This edited volume owes a debt of gratitude to 49 contributors from institutions across academia, national laboratories, and industry. The three editors were fortunate to receive an outstanding collection of contributions from leading researchers on a myriad of topics within the homeland security risk and decision analysis space. The editors also thank the management within the National Security Directorate at Pacific Northwest National Laboratory for encouraging and supporting the development of this volume. This edited volume is organized into 4 thematic parts/sections with 19 total chapters based on DHS's missions: (i) "Managing National Security Risk and Policy Programs," (ii) "Strengthening Ports of Entry," (iii) "Securing Critical Cyber Assets," and (iv) "Enhancing Disaster Preparedness and Infrastructure Resilience."

Part I contains five chapters: Chapter 1 "On the 'Influence of Scenarios to Priorities' in Risk and Security Programs" by Thorisson and Lambert from the University of Virginia, Chapter 2 "Survey of Risk Analytic Guidelines Across the Government" by Maya et al. from the University of Southern California, Chapter 3 "An Overview of Risk Modeling Methods and Approaches for National Security" by Chatterjee et al. from the Pacific Northwest National Laboratory, Chapter 4 "Comparative Risk Rankings in Support of Homeland Security Strategic Plans" by Lundberg from Sam Houston State University, and Chapter 5 "A Data Science Workflow for Discovering Spatial Patterns Among Terrorist Attacks and Infrastructure" by Fortin et al. from the Pacific Northwest National Laboratory.

Part II contains three chapters: Chapter 6 "Effects of Credibility of Retaliation Threats in Deterring Smuggling of Nuclear Weapons" by Shan and Zhuang from the State University of New York at Buffalo, Chapter 7 "Disutility of Mass Relocation After a Severe Nuclear Accident" by Bier and Liu from the University of Wisconsin–Madison, and Chapter 8 "Scheduling Federal Air Marshals Under Uncertainty" by DeGregory and Ganesan from US Military Academy and George Mason University, respectively.

Part III contains three chapters: Chapter 9 "Decision Theory for Network Security: Active Sensing for Detection and Prevention of Data Exfiltration" by McCarthy et al. from the University of Southern California and Hewlett Packard Labs, Chapter 10 "Measurement of Cyber Resilience from an Economic Perspective" by Rose and Miller from the University of Southern California, and Chapter 11 "Responses to Cyber Near-Misses: A Scale to Measure Individual Differences" by Cui et al. from the University of Southern California.

Part IV contains eight chapters: Chapter 12 "An Interactive Web-Based Decision Support System for Mass Dispensing, Emergency Preparedness, and Biosurveillance" by Lee et al. from Georgia Institute of Technology and Centers for Disease Control and Prevention, Chapter 13 "Measuring Critical Infrastructure Risk, Protection, and Resilience in an All-Hazards Environment" by Phillips and Petit from the Perduco Group and Argonne National Laboratory, respectively, Chapter 14 "Risk Analysis Methods in Resilience

Modeling: An Overview of Critical Infrastructure Applications” by Baroud from Vanderbilt University, Chapter 15 “Optimal Resource Allocation Model to Prevent, Prepare, and Respond to Multiple Disruptions, with Application to the Deepwater Horizon Oil Spill and Hurricane Katrina” by MacKenzie and Al-Kazimi from the Iowa State University, Chapter 16 “Inoperability Input–Output Modeling of Electric Power Disruptions” by Santos et al. from George Washington University and University of Massachusetts–Lowell, Chapter 17 “Quantitative Assessment of Transportation Network Vulnerability with Dynamic Traffic Simulation Methods” by Shekar and Fiondella from the University of Massachusetts–Dartmouth, Chapter 18 “Infrastructure Monitoring for Health and Security” by Basu from Vanderbilt University, and Chapter 19 “Exploring Metaheuristic Approaches for Solving the Traveling Salesman Problem Applied to Emergency Planning and Response” by Tipireddy et al. from the Pacific Northwest National Laboratory and St. Mary’s University.

Richland, WA, USA
26 November 2018

*Samrat Chatterjee, Robert T. Brigantic
and Angela M. Waterworth*
National Security Directorate
Pacific Northwest National Laboratory

Chapter Abstracts

Chapter 1 – Page 3 (Thorisson and Lambert)

On the “Influence of Scenarios to Priorities” in Risk and Security Programs

Organizations increasingly follow comprehensive guidelines and standards when implementing programs for the assessment and management of risk, safety, resilience, or security. Programs often involve the coordination of multiple systems, of stakeholders and organizational units, and require balancing different needs and missions, as well as being flexible and having the ability to withstand and adjust to emerging conditions of economics, policies, military conflict, environment, and other factors. This chapter suggests three canonical questions as the mission of such a program: (i) what sources of risks are to be managed by the program; (ii) how should multiple risk assessment, risk management, and risk communication activities be administered and coordinated, and what should be the basis for resource allocation to these activities; and (iii) how will the performance of the program be monitored and evaluated. An approach to evaluate how different components of a program comply with guidelines and how various risk scenarios influence the priorities of the program is demonstrated. Thus, it emphasizes the preparedness of programs whose priorities adjust to emergent conditions of technology, environment, demographics, markets, regulations, organizations, and geography. The methods presented are useful to organizations and agencies implementing risk guidelines for security, infrastructure, finance, logistics, emergency management, resilience, and preparedness.

Chapter 2 – Page 25 (Maya, Liu, Zhu, Tran, Creighton and Woo)

Survey of Risk Analytic Guidelines Across the Government

The Department of Homeland Security (DHS) has been developing its guidance for standardizing risk analyses practices to facilitate high quality, data fidelity, utility of results, and appropriate consistency for the analyses performed by