CONTENTS

Contributors xv
Acknowledgments xxiii
Foreword xxv
   Richard A. Falkenrath
Preface xxix
   David G. Kamien
Introduction: Homeland Security in Context xli
   David G. Kamien

SECTION ONE AL-QAIDA AND GLOBAL JIHAD

Chapter 1
Introduction to Section 1 3
   Rohan Kumar Gunaratna

Chapter 2
Al-Qaida: Origins, Goals, and Grand Strategy 9
   Ahmed S. Hashim

Chapter 3
The Role of Islam as a Motivating Factor in Usama bin Ladin’s Appeal within the Muslim World 37
   David Cook

Chapter 4
Understanding al-Qaida Networks 53
   Marc Sageman

Chapter 5
Al-Qaida: Terrorist Selection and Recruitment 73
   Scott Gerwehr and Sara Daly
Chapter 6
“The War of the Ether”: Al-Qaeda’s Psychological Warfare Campaign Against the Western and Muslim Worlds  91
Michael G. Knapp

SECTION TWO TERRORISM BEYOND AL-QAIDA

Chapter 7
Introduction to Section 2  115
Noel Koch

Chapter 8
The New Age of Terrorism  117
Brian Michael Jenkins

Chapter 9
Chaos, Terrorism, and Beyond  131
Xavier Raufer

Chapter 10
The Psychology of Terrorism: Future Directions and Potential Implications for Counterterrorist Policy  143
John Horgan

Chapter 11
WMD and Lessons from the Anthrax Attacks  157
Leonard A. Cole

Chapter 12
Biological Terrorism: Risks and Responses  175
Terrence M. O’Sullivan

Chapter 13
Hizballah  195
Daniel Byman
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Terrorist Financing</td>
<td>207</td>
</tr>
<tr>
<td></td>
<td>Steve Emerson</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SECTION THREE THE ROLE OF GOVERNMENT</strong></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Introduction to Section 3</td>
<td>223</td>
</tr>
<tr>
<td></td>
<td>Susan M. Collins</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Homeland Security’s National Strategic Position: Goals, Objectives,</td>
<td>225</td>
</tr>
<tr>
<td></td>
<td>Measures Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sharon L. Caudle and Randall Yim</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Congressional Oversight over Homeland Security and the Dynamics of</td>
<td>263</td>
</tr>
<tr>
<td></td>
<td>Appropriation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Christopher Shays</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>The Department of Defense: Defending the Homeland and Defeating</td>
<td>283</td>
</tr>
<tr>
<td></td>
<td>Enemies Abroad</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paul McHale</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Emergency Planning: The Evolving Role of Regional Planning</td>
<td>297</td>
</tr>
<tr>
<td></td>
<td>Organizations in Supporting Cities and Counties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>David Robertson</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Preparing a City for Terrorism</td>
<td>311</td>
</tr>
<tr>
<td></td>
<td>Martin O’Malley</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Legal Issues</td>
<td>325</td>
</tr>
<tr>
<td></td>
<td>Michael Kraft</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 22
Transatlantic Counterterrorism: Some Recommendations 347
Karen J. Greenberg

Chapter 23
International Cooperation in Counterterrorism 353
Gijs de Vries

SECTION FOUR COUNTERTERRORISM INTELLIGENCE AND ANALYSIS

Chapter 24
Introduction to Section 4 361
Sidney J. Caspersen

Chapter 25
A Typology and Anatomy of Terrorist Operations 365
Dennis A. Pluchinsky

Chapter 26
Intelligence and Information Sharing in Counterterrorism 391
C. Patrick Duecy

Chapter 27
Counterterrorism Analysis and Homeland Security 413
Mark V. Kauppi

SECTION FIVE RISK: MANAGEMENT, PERCEPTION, AND COMMUNICATION

Chapter 28
Introduction to Section 5 429
Anthony Beverina
Chapter 29
Integrating Risk Management with Security and Antiterrorism Resource Allocation Decision Making 431
Gregory S. Parnell, Robin L. Dillon-Merrill, and Terry A. Bresnick

Chapter 30
The Psychological Perception of Risk 463
Baruch Fischhoff

Chapter 31
The Homeland Security Advisory System 493
James Jay Carafano

Chapter 32
The Role of Broadcast Media in Homeland Security Communication 505
Frank Sesno

SECTION SIX SECURING CRITICAL INFRASTRUCTURE AND CYBERSPACE

Chapter 33
Introduction to Section 6 519
James F. McDonnell

Chapter 34
Critical Infrastructure and Interdependency 523
Rae Zimmerman

Chapter 35
Cybersecurity in Post-9/11 America 547
James D. Cunningham

SECTION SEVEN BORDER AND TRANSPORTATION SECURITY

Chapter 36
Introduction to Section 7 583
William H. Parrish
Chapter 37
Border Control  587
   K. Jack Riley

Chapter 38
Civil Aviation in the United States: Security Before and After 9/11  613
   Cathal “Irish” Flynn and Art Kosatka

Chapter 39
Port and Maritime Security  631
   Carl Bentzel

Chapter 40
Transportation Information and Security  649
   Harold W. Neil, Jr.

SECTION EIGHT EMERGENCY MANAGEMENT, PUBLIC HEALTH, AND MEDICAL PREPAREDNESS

Chapter 41
Introduction to Section 8  661
   Donna F. Barbisch

Chapter 42
Emergency Response: An Overview  665
   Ray Lehr

Chapter 43
National Response Plan, the National Incident Management System, and the Federal Response Plan  677
   Claire B. Rubin and John R. Harrald

Chapter 44
Understanding and Preparing for the Psychological Consequences of Terrorism  689
   Terri L. Tanielian and Bradley D. Stein
Chapter 53
Legal Issues for Business in Responding to Terrorist Events  845
William C. Nicholson

SECTION TEN ACADEME

Chapter 54
Introduction to Section 10  863
Scott D. Bates

Chapter 55
Academe and Homeland Security  865
Todd I. Stewart

Chapter 56
Considering a New Paradigm for Strategic Studies  899
Joseph E. Vorbach III and Patrick N. Newman

Chapter 57
Decision Models for Emergency Response Planning  911
Richard C. Larson

SECTION ELEVEN SCIENCE, TECHNOLOGY, AND INFORMATION SHARING

Chapter 58
Introduction to Section 11  931
Terry Janssen

Chapter 59
Science, Technology, and Terrorism  933
Thurman J. Allard and Nigel Hey

Chapter 60
Improving Checkpoint Security  957
Fred Facemire and Mark Laustra
Chapter 61
IT Architecture for Homeland Security  969
    Gerald Metz

Chapter 62
Two Critical Concepts for Information Technology in Homeland Security  985
    Don Adams

Chapter 63
Needs Analysis for Information Sharing  999
    David G. Kamien, Jean-Francois Cloutier, and Denis Ranger

SECTION TWELVE DOMESTIC SECURITY AND CIVIL LIBERTIES

Chapter 64
Introduction to Section 12  1009
    K. A. Taipale

Chapter 65
Thinking About Civil Liberty and Terrorism  1013
    Paul Rosenzweig

Chapter 66
Security and Freedom of Speech  1031
    Abraham H. Foxman

Chapter 67
Principled Prudence: Civil Liberties and the Homeland Security Practitioner  1045
    Laura W. Murphy

Chapter 68
Government Data Mining  1063
    Newton N. Minow and Fred H. Cate
SECTION THIRTEEN POLITICS AND ACCOUNTABILITY

Chapter 69
Introduction to Section 13  1089
   Warren Rudman

Chapter 70
The Politics of Homeland Security  1091
   Anne M. Khademian

Chapter 71
Accountability and Homeland Security  1115
   Charles R. Wise and Rania Nader

Chapter 72
Waging the “War of Ideas”  1131
   William Rosenau

Glossary  1149

Index  1157
CONTRIBUTORS

Don Adams  VP, Chief Technology Officer–Government and Chief Security Officer, TIBCO Software (CHAP. 62)

Thurman J. Allard  Director of Homeland Security, Sandia National Laboratories (CHAP. 59)

Major General Donna F. Barbisch, C.R.N.A., M.P.H., D.H.A.  Director, Chem Bio Radiological and Nuclear Defense Programs Integration, Department of Defense; Adjunct Professor, George Washington University; President, Global Deterrence Alternatives, LLC (CHAP. 41)

The Honorable Scott D. Bates, J.D.  Senior Fellow, Center for National Policy; Former Senior Policy Advisor, U.S. House Select Committee on Homeland Security (CHAP. 54)

Carl Bentzel, J.D., LL.M.  Advisor for Homeland Security, DCI Group LLC; Former Senior Advisor, U.S. Senate Committee on Commerce, Science, and Transportation Committee (CHAP. 39)

Anthony Beverina  President and Chief Operating Officer, Digital Sandbox, Inc. (CHAP. 28)

Mark Braverman, Ph.D.  Prinicipal, The Braverman Group, LLC (CHAP. 51)

Terry A. Bresnick  President and Senior Principal, Innovative Decisions, Inc. (CHAP. 29)

Dr. Daniel Byman  Associate Professor, Walsh School of Foreign Service, Georgetown University; Nonresident Senior Fellow, Saban Center for Middle East Policy, Brookings Institution (CHAP. 13)

Dr. James Jay Carafano  Senior Fellow, The Heritage Foundation (CHAP. 31)

Sidney J. Caspersen  Director, Office of Counter-Terrorism, State of New Jersey (CHAP. 24)
Fred H. Cate, J.D.  Distinguished Professor and Director, Center for Applied Cybersecurity Research, Indiana University; Senior Policy Advisor, Center for Information Policy Leadership at Hunton and Williams (CHAP. 68)


Jean-Francois Cloutier  CTO, Mind-Alliance Systems (CHAP. 63)

Leonard A. Cole, Ph.D.  Adjunct Professor, Department of Political Science, Rutgers University (CHAP. 11)

Senator Susan M. Collins  Chairman U.S. Senate Committee on Homeland Security and Governmental Affairs (CHAP. 15)

David Cook, Ph.D.  Assistant Professor, Department of Religious Studies, Rice University (CHAP. 3)

James D. Cunningham  Science Applications International Corporation (SAIC) (CHAP. 35)

Sara Daly  International Policy Analyst, The RAND Corporation (CHAP. 5)

Gijs de Vries  Counterterrorism Coordinator, European Union (CHAP. 23)

Dr. Robin L. Dillon-Merrill  Professor, Georgetown University; Principal, Innovative Decisions, Inc. (CHAP. 29)

William Donnelly  Chairman, Morris County Infrastructure Advisory Group (CHAP. 52)

C. Patrick Duecy  Partner, Homeland Solutions, LLC. (CHAP. 26)

Steve Emerson  Executive Director, The Investigative Project on Terrorism (CHAP. 14)

Fred Facemire  Director, System Integration, Smiths Detection (CHAP. 60)

Richard A. Falkenrath, Ph.D.  Senior Fellow, Foreign Policy Studies, The Brookings Institution; Former White House Deputy, Homeland Security Advisor (FOREWORD)
Contributors

Dr. Baruch Fischhoff Howard Heinz University Professor, Department of Social and Decision Sciences, Carnegie Mellon University (CHAP. 30)

Admiral Cathal “Irish” Flynn (Retired) TranSecure, Inc. (CHAP. 38)

Abraham H. Foxman National Director, Anti-Defamation League (CHAP. 66)

Scott Gerwehr Associate Policy Analyst, The RAND Corporation (CHAP. 5)

Governor James Gilmore Partner, Kelley Drye & Warren LLP (CHAP. 47)

Karen J. Greenberg Executive Director, Center on Law and Security, New York University (CHAP. 22)

Rohan Kumar Gunaratna, Ph.D. Head of Terrorism Research and Associate Professor, Institute for Defense and Strategic Studies, Singapore (CHAP. 1)

Elin A. Gursky, Sc.D. Principal Deputy for Biodefense, National Strategies Support Directorate, ANSER/Analytic Services, Inc. (CHAP. 45)

Jack R. Harrald, Ph.D. Codirector, George Washington University, Institute for Crisis, Disaster, and Risk Management (CHAP. 43)

Ahmed S. Hashim, Ph.D. Professor of Strategic Studies, United States Naval War College (CHAP. 2)

Nigel Hey Sandia National Laboratories (CHAP. 59)

John Horgan, Ph.D. C. Psychol., Lecturer, Department of Applied Psychology, University College, Cork, Ireland (CHAP. 10)

Terry Janssen Chief Technologist for Knowledge Management, Lockheed Martin Corporation (CHAP. 58)

Brian Michael Jenkins Senior Advisor to the President of The RAND Corporation; Director of the National Transportation Security Center at the Mineta Transportation Institute (CHAP. 8)

David G. Kamien CEO, DGK LLC Homeland Security Management Consulting (INTRODUCTION and CHAP. 63)
Mark V. Kauppi  Program Director, Counterterrorism Training for Analysts, Joint Military Intelligence Center, U.S. Army (CHAP. 27)

Ronald J. Kelly  Director, IBM Corporate Security (CHAP. 48)

Anne M. Khademian  Associate Professor, Center for Public Administration and Policy, Virginia Polytechnic University (CHAP. 70)

Michael G. Knapp  Middle East Analyst, U.S. Army National Guard Intelligence Center (CHAP. 6)

Noel Koch  Chairman and CEO, TranSecur, Inc.; Former Director of Special Planning, U.S. Department of Defense; Former Special Assistant to the President (CHAP. 7)

Art Kosatka  CEO, TranSecure, Inc. (CHAP. 38)

Michael Kraft  Counterterrorism Consultant; Former Senior Advisor for Legislative and Budget Affairs in the State Department Office of the Coordinator for Counterterrorism; Former Staff Director of the Senate Foreign Relations Committee Middle East Subcommittee (CHAP. 21)

Richard C. Larson, Ph.D.  Professor of Civil and Environmental Engineering and of Engineering Systems, Massachusetts Institute of Technology (CHAP. 57)

Mark Laustra  Smiths Detection (CHAP. 60)

Ray Lehr  Northrop Grumman Corporation, Assistant Chief (Retired), Baltimore City Fire Department (CHAP. 42)

James F. McDonnell  Vice President and Chief Information and Security Officer, USEC, Inc. (CHAP. 33)


Gerald Metz  Chief Engineer, C2 Infrastructure Programs, Northrop Grumman Mission Systems (CHAP. 61)

Newton N. Minow  Senior Counsel, Sidley Austin Brown and Wood (CHAP. 68)

Laura W. Murphy  Director, Washington Legislative Office, American Civil Liberties Union (ACLU) (CHAP. 67)
Contributors

Rania Nader  School of Public and Environmental Affairs, Indiana University (CHAP. 71)

Harold W. Neil, Jr.  Executive Assistant, Office of Transportation Security, Department of Transportation, State of New Jersey (CHAP. 40)

Patrick N. Newman, J.D.  Program Manager, Marine Transportation System Initiative, U.S. Coast Guard Academy (CHAP. 56)

William C. Nicholson, Esq.  Adjunct Professor, Widener University School of Law (CHAP. 53)

The Honorable Martin O'Malley  Mayor, City of Baltimore, Maryland (CHAP. 20)

Alan Orlob  Vice President, Corporate Security, Marriott International Lodging (CHAP. 50)

Terrence M. O'Sullivan  Homeland Security Center for Risk and Economic Analysis (CREATE), University of Southern California (CHAP. 12)

William H. Parrish  Associate Professor, L. Douglas Wilder School of Government and Public Affairs, Virginia Commonwealth University (CHAP. 36)

Dr. Gregory S. Parnell  Professor of Systems Engineering, United States Military Academy at West Point; Senior Principal, Innovative Decisions, Inc. (CHAP. 29)

Dennis A. Pluchinsky  Senior Threat Analyst, TranSecur, Inc.; Terrorism Analyst, U.S. Department of State (Retired) (CHAP. 25)

Dr. Lion Poles  Deputy Director General, Kaplan Medical Center (CHAP. 46)

Denis Ranger  Product Architect, Mind-Alliance Systems (CHAP. 63)

Xavier Raufer  Director of Studies, Department for the Study of the Contemporary Criminal Menace, Criminology Institute, University of Paris II–Panthéon-Assas (CHAP. 9)

K. Jack Riley  Associate Director of RAND, Infrastructure, Safety, and Environment, The RAND Corporation (CHAP. 37)
Contributors

**David Robertson**  Executive Director, Metropolitan Washington Council of Governments (CHAP. 19)

**William Rosenau**  Political Scientist, The RAND Corporation, Washington Office; Adjunct Professor, Security Studies Program, Georgetown University (CHAP. 72)

**Paul Rosenzweig**  Senior Legal Research Fellow, The Heritage Foundation, Adjunct Professor of Law, George Mason University, School of Law (CHAP. 65)

**Claire B. Rubin**  President and Principal, Claire B. Rubin & Associates, Disaster Research and Consulting; Senior Research Scientist, George Washington University, Institute for Crisis, Disaster, and Risk Management (CHAP. 43)

**The Honorable Warren Rudman**  Counsel, Paul, Weiss, Rifkind, Wharton & Garrison LLP; Former U.S. Senator from New Hampshire (CHAP. 69)

**Marc Sageman, M.D., Ph.D.**  Senior Fellow, Foreign Policy Research Institute; Lecturer, Solomon Asch Center for the Study of Ethnopolitical Conflict, University of Pennsylvania (CHAP. 4)

**Donald L. Schmidt**  Emergency Response Planning Practice Leader, Marsh Risk Consulting (CHAP. 49)

**Frank Sesno**  Professor of Public Policy and Communication, School of Public Policy, George Mason University; CNN Special Correspondent (CHAP. 32)

**Shmuel C. Shapira, M.D.**  Deputy Director General, Hadassah Medical Organization (CHAP. 46)

**Congressman Christopher Shays**  Chairman, House Subcommittee on National Security, Emerging Threats, and International Relations (CHAP. 17)

**Bradley D. Stein, M.D., Ph.D., M.P.H.**  Natural Scientist, Associate Director for Mental and Behavioral Health, Center for Domestic and International Health Security, The RAND Corporation (CHAP. 44)

**Todd I. Stewart**  Major General U.S. Air Force (Retired); Executive Director, National Academic Consortium for Homeland Security (CHAP. 55)
Contributors

Dr. Boaz Tadmor   Director, Cerberus Enterprises, LLC (CHAP. 46)

K. A. Taipale   Executive Director, Center for Advanced Studies in Science and Technology Policy, World Policy Institute (CHAP. 64)

Terri L. Tanielian, M.A.   Senior Research Analyst, Associate Director for Mental and Behavioral Health, Center for Domestic and International Health Security, The RAND Corporation (CHAP. 44)

Commander Joseph E. Vorbach III, Ph.D.   Associate Professor of International Relations and Director, Marine Transportation System Initiative, U.S. Coast Guard Academy (CHAP. 56)

Charles R. Wise   Professor, School of Public and Environmental Affairs, Indiana University (CHAP. 71)

Randall Yim, Esq.   Director, Homeland Security Institute (CHAP. 16)

Rae Zimmerman, Ph.D.   Professor of Planning and Public Administration; Director, Institute for Civil Infrastructure Systems (ICIS), Wagner Graduate School of Public Service, New York University (CHAP. 34)
ACKNOWLEDGMENTS

My deep thanks go to the contributors whose introductions, chapters, and illustrations make up The McGraw-Hill Handbook of Homeland Security. I am also grateful for the expert editorial assistance provided by Susan Gamer, Aileen Torres, and my publisher: Jeffrey Krames, Laura Libretti, Maureen Walker, and the rest of the staff at McGraw-Hill.

I received many forms of assistance and encouragement from a great many institutions and people, including David Afhauser, Victor Anderes, Caroline Barnes, Mia Bloom, Sharon Caudle, Elizabeth Clausen, Jean-François Cloutier, Elissa Davidson, Amanda Dory, Lee Ewing, Al Felzenberg, Larry Halloran, Michael Hopmeier, Rosanne Hynes, Andrew Lauland, Don Kettl, Anna Khademian, Ray Lehr, Tony Moore, Harold Neil, John Paczkowski, Brad Penuel, Bob Poole, Tim Raducha-Grace, Edna Reid, Lisa Shields, Matthew Statler, Howard Steinberg, Paul Wilkinson, Dave Zolet, and others.

Several of the contributors—Mike Kraft, Claire Rubin, Dennis Pluchinsky, and Jack Riley—were exceptionally helpful in introducing me to other contributors and providing feedback. They deserve special thanks.

I also appreciate the efforts of government employees and the staff of the 9/11 Commission, and the work of numerous think tanks and task forces that have studied terrorism, have worked in the area of homeland security, and have passed on their knowledge in reports and studies.

The warm support provided by my wife, Felice Maranz; my children, Daniel and Amalia; and my parents, Anita and Roger Kamien, was essential to the completion of this book, and I dedicate it to them with love.
Before the terrorist attacks of 9/11, there was no field called “homeland security” and hence no need for a handbook such as this. Today, homeland security is a multibillion-dollar enterprise and the motivating force behind countless reforms across dozens of heretofore separate government activities. The need for this enterprise is not tied to the fate of al-Qaida or any other particular terrorist group; instead, it derives from the structural—and hence, for all intents and purposes, permanent—vulnerability of free and open societies to catastrophic terrorist attacks. This vulnerability existed before 9/11 and will continue to exist indefinitely. Because all governments are charged with safeguarding their civilian population from deliberate large-scale death and destruction, homeland security has become a permanent mission for responsible governments worldwide.

Homeland security is a composite of many different fields that individually have some bearing on the terrorist threat to modern societies, the vulnerability of these societies to various forms of terrorist attack, and the techniques to combat these threats and vulnerabilities. Each individual field is supported by the knowledge and experience of an established community of experts and practitioners. As yet there is no community of individuals with the interdisciplinary breadth needed to manage the field of homeland security comprehensively and effectively.

The contrast between homeland security and national security (another even broader interdisciplinary field) is instructive. National security describes many different kinds of measures—diplomatic, economic, military, covert, overt, legal, illegal, etc.—taken by a state to ensure its survival and security. National security has been practiced by governments for centuries, and over time has emerged as a distinct field supported by a community of individuals with
similar educational and practical backgrounds. Individuals from this community are able to coalesce quickly into effective work groups because they share a frame of reference, an understanding of established national security processes, and a general familiarity with each other’s areas of profound expertise. This collection of national security experts represents what social scientists call an “epistemic community.”

Homeland security has no epistemic community to speak of, but needs one. Men and women from dozens of different disciplines—regional experts, terrorism analysts, law enforcement officials, intelligence officers, privacy specialists, diplomats, military officers, immigration specialists, customs inspectors, specific industry experts, regulatory lawyers, doctors and epidemiologists, research scientists, chemists, nuclear physicists, information technologists, emergency managers, firefighters, communications specialists, and politicians, to name a few—are currently involved in homeland security, but it is not enough merely to aggregate specialists. The tendency to organize around disciplines, to adopt “stovepiped” approaches to problems, and to optimize solutions for part but not all of the problem is too strong among loose collections of unadulterated specialists. Only a team of individuals with genuine crosscutting knowledge and experience will be able to understand the complexity of any particular homeland security challenge, devise an efficient and viable strategy for dealing with the problem, and implement this strategy effectively.

There is an acute national and indeed international need for professionals who can think and operate across the breadth of homeland security while at the same time contributing expertise in one or more of the disciplines that comprise the field as a whole. There are only a few such individuals today, so more must be trained. Governments worldwide have already created a demand for such individuals, but the educational system in the United States has only just begun to provide the knowledge base and training capabilities needed to meet the government’s demand for the genuine homeland security professional. Educational systems outside the United States are even farther behind.

This volume is long, and for a reason: its length is indicative of the substantive breadth of homeland security itself. Each individual chapter deals with a different and important aspect of the field as a whole. Together, the chapters provide a first-rate overview of a new and exceedingly complex field—a perspective that is broad, deep, and
cognizant of the interrelationships among the disparate disciplines that make up homeland security. In that respect, this handbook is the first of its kind and an invaluable resource.

This handbook represents an important step toward creating the professional community that governments require to implement a comprehensive homeland security agenda effectively and efficiently. As such, the book makes a rare contribution not just to a professional literature but also to a noble public purpose: securing a nation from catastrophic terrorist attack while preserving the freedom and openness that make the homeland vulnerable in the first place.
PREFACE

The McGraw-Hill Handbook of Homeland Security takes a broad view of the challenges involved in enhancing domestic security and emergency preparedness. Our goal is to contribute to the discussion of this national issue and heighten readers’ awareness of the importance of integrating policies, strategies, and initiatives across different areas into a cohesive national and international effort.

The book provides a comprehensive introduction to the subject for university students, policy makers, and industry professionals. Several assumptions underlie the selection of chapters. First, although homeland security and national preparedness now encompass “all hazards,” including events such as natural disasters, the focus of the book is on terrorism and security, areas where an understanding of the human element of the terrorist threat is critical. Second, with or without Usama bin Laden as its leader, al-Qaida and radical fundamentalist Islam will remain a threat. An entire section is devoted to understanding this dominant terror threat to the United States. Third, regardless of specific types of attacks and the affiliation of their perpetrators, many of the principal missions and challenges that homeland security policy makers, operational managers, and analysts face will remain the same.

KEY FEATURES

The McGraw-Hill Handbook of Homeland Security has several important features:

- The text provides extensive thematic coverage, encompassing analysis of al-Qaida and related terrorist threats, and of homeland security as part of the United States’ response. There are more than 70 original chapters and case studies about a wide range of subjects, providing an opportunity to understand how homeland security challenges are interconnected. The book is the first in the literature to combine such
a comprehensive array of topics, creating a basis for a shared understanding of homeland security.

- The contributors include distinguished members of Congress; senior federal, state, and local government officials; industry professionals; and academics, many of whom combine theory with practical experience in homeland security and are active in educating the next generation of national security leaders.

- The book includes chapters on practical matters and chapters that present theoretical models and concepts.

- The book covers recent developments, such as the July 2005 bombing in London and the restructuring of the Department of Homeland Security as a result of the Second Stage Review initiated by Secretary Chertoff, the Intelligence Reform and Terrorism Prevention Act of December 2004, the vote to create a permanent Committee on Homeland Security, and the appointment of Michael Chertoff as the secretary of the Department of Homeland Security.


ORGANIZATION

This book is divided into 13 sections, each preceded by a brief introduction to set the stage for the chapters that follow. These sections group the components of what many consider core homeland security subject matter into thematic units that provide a framework for study and discussion. Preceding Section 1 is an introductory chapter, “Homeland Security in Context,” that places the subject in the setting of other policy frameworks and identifies some of its principal components.

Section 1: Al-Qaida and Global Jihad

In order to confront the threat posed by Usama bin Ladin, the al-Qaida network, and affiliated fundamentalist Islamist terrorist groups, one must understand their ideology, vision, strategy, recruiting methods, and use of the Internet. Al-Qaida’s goals are to force occupying “infidels” off Muslim land; topple illegitimate apostate Arab regimes; drive U.S. forces out of Iraq, Saudi Arabia,
and Afghanistan; and destroy Israel. Jihadists see their effort as an apocalyptic struggle, a righteous war of defense of the very existence of Islam and the Muslim world from attack and disintegration by a Zionist-Crusader conspiracy of infidels—Israel and the Jews, America, and “puppet” secular Arab regimes.

The most profound development related to al-Qaida since 9/11 is its transformation from a group to the self-proclaimed vanguard of Islamic movements, galvanizing Islamists worldwide to fight two battles: against their own governments and against the United States and its allies. Many extremist Muslims see bin Ladin as a figure of hope who can restore their dignity and save the Islamic world. According to bin Ladin’s interpretation of the Muslim religion and its history, a violent jihad is justified and indeed noble.

The main Islamist terrorist threat to the United States comes not from a monolithic al-Qaida organization but from the broader, violent Islamist revivalist social movement, united by bin Ladin’s utopian vision of justice and fairness. The threat from al-Qaida and its affiliates will remain even if bin Ladin is killed; and several of the contributors to this book think that the threat has been nourished by conflict in Iraq.

By analyzing biographical data on the terrorists and the topology of Islamist terrorist networks, as is done in one chapter, one can better understand how and why people join Islamist terror networks. For instance, one chapter in Section 1 describes various models al-Qaida may be using to recruit new members, including the “net,” “funnel,” “infection,” and “seed crystal,” along with psychographic or “state” factors. This section also explains how the Internet is central to the strategy of al-Qaida and the global jihad, which clearly appreciate its value as a weapon of psychological warfare, perception management, recruitment, and fund-raising.

Section 2: Terrorism Beyond al-Qaida

The second section looks beyond the topic of al-Qaida to study terrorism as a phenomenon, associated threats, and other groups. There is no universal definition of terrorism; rather, terrorism is a generalized construct derived from our concepts of morality, law, and the rules of war. Terrorism is a hugely complex social problem—what we see in an attack is only the tip of the iceberg—which must be
understood in a broad sociocultural global context of chaos at the intersection of lawless places, dangerous flows, and extreme ideology.

Terrorism is an “asymmetric” form of warfare: a low-cost means of attacking civilian populations and national infrastructures when the enemy has superior economic and military might and therefore cannot be struck at with conventional tactics and weapons. However, terrorism is not only a matter of physical attacks but it is a mental game used to erode citizens’ morale and their faith in their government, and to demonstrate strength to the terrorists’ constituencies.

Important trends in terrorism over the past decades are presented in Section 2, but readers are cautioned against forecasting by extrapolation. Terrorist groups vary in culture, ideology, and priorities. Tomorrow’s terrorism will surely be different from today’s; and even at present it is misleading to lump all groups that use terrorist tactics into a notionally homogeneous group called “terrorists.” This section includes a chapter on Hizballah, which aspires to transform Lebanon into an Islamic state and receives funding, training, and intelligence from Iran, a country that depicts the United States as the “great Satan” and aspires to build nuclear weapons. Readers are also presented with some of the limitations of psychology in understanding terrorists and terrorism. One chapter discusses terrorists’ financing and efforts to counter it.

Another topic addressed in Section 2 is perhaps the most troubling terrorist threat: weapons of mass destruction (WMD) such as nuclear bombs, as well as weapons of mass effect such as biological and chemical agents and radiological dispersal devices (dirty bombs). Although attacks with unconventional weapons are relatively rare compared to attacks using explosives, and despite the fact that the “anthrax letters” of October 2001 resulted in only five fatalities, the possibility of WMD attacks implies a need for constant vigilance. Therefore, this section analyzes biological weapons in some detail, discussing their history and considering their potential future use by terrorists.

**Section 3: The Role of Government**

Section 3 introduces the role of various levels of government in homeland security. For the federal government, homeland security is a complex set of overlapping national missions. One chapter
recommends ways to build capabilities and develop oversight so as to achieve those missions. Other chapters discuss the roles of the House and Senate (which not only exercise oversight but are of course responsible for federal appropriations for homeland security) and the Department of Defense (in this regard, one chapter describes the mission of the Northern Command and National Guard). The section also takes up regional planning organizations in cities and counties, which provide important support to the federal and state governments in homeland security management. Municipalities are likely to bear the brunt of terrorist attacks because such attacks typically occur in cities. At the municipal level, the primary challenges have to do with managing first responders: firefighters, police, emergency medical services, and citizens.

Still other chapters in Section 3 discuss law and intergovernmental counterterrorism. Terrorism has traditionally been addressed in the international community with treaties, such as those condemning hijacking and hostage-taking. One chapter considers new legal instruments such as the PATRIOT Act, emphasizing the need for effective, concerted implementation. Another chapter suggests that the United States could learn lessons about counterterrorism from Europe. It is also important to establish communication channels with foreign countries to share information and to foster trust and personal working relationships. Strategies for apprehending terrorists, such as standards and norms for extradition, should also be established internationally. One chapter stresses the importance of frameworks for international cooperation provided by the European Union and the United Nations. Ultimately, there can be no homeland security without international security.

Section 4: Counterterrorism Intelligence and Analysis

Arguably, counterterrorism must begin with analysis. In Section 4, one chapter provides a valuable typology of terrorism and an anatomy of the stages in planning offensive or logistical operations, although the reader is cautioned that despite any similarities in weapons and tactics, each terrorist offensive is unique. Another analysis in this section contrasts intelligence during the Cold War with intelligence today, when the intelligence community must deal with global, transnational groups that are difficult to detect, observe,
and counter. With responsibility for different functions and phases of the intelligence cycle divided among many agencies, cooperation and information sharing must override bureaucratic turf wars. The Intelligence Reform and Terrorism Prevention Act of 2004 aims to align the 15 agencies of the intelligence community to achieve effective counterterrorism, but the unique bureaucratic culture of these semiautonomous agencies remains a formidable obstacle to cooperation. In one chapter, readers will be introduced to a five-step “intelligence process” and will learn that we actually have too much, not too little, intelligence—and that intelligence analysts must determine what information to feed into the process. The need for information sharing is emphasized, and the expanded role of law enforcement since 9/11 is addressed.

Section 5: Risk: Management, Perception, and Communication

The introduction to Section 5 notes that risk management is a never-ending process. Efforts made to achieve security and preparedness must be adjusted to changing levels of threat. One chapter in this section explores decision-making frameworks for antiterrorism planning, development, and implementation, including resource allocation; the authors maintain that risk assessment and risk management must accord with an organization’s broader goals, objectives, and missions. To support their decisions, organizations need an unbiased, traceable process based on techniques of decision making and risk analysis.

Communicating warnings and other information about risks requires considerable sensitivity. Terrorism is meant to instill fear and anxiety; thus leaders must communicate in ways that inspire confidence, demonstrating that risk is being well managed. Citizens must trust their government enough to listen to its messages and respond effectively. How officials manage and communicate risk in a crisis will determine citizens’ reaction to future communications. One chapter in this section examines the Homeland Security Advisory System (HSAS), which issues color-coded warnings. The broadcast media also play a significant role in disseminating information to the public. As is noted in one chapter, public officials need to be fluent in the “language of live”—that is, live broadcasting—so as to convey information
about unfolding, confusing situations as clearly, transparently, and calmly as possible.

**Section 6: Securing Critical Infrastructure and Cyberspace**

In order to secure critical infrastructure, one must know what constitutes infrastructure, what makes it critical, and what functions of critical infrastructure are interdependent. Section 6 includes that information; it also provides a historical context for the evolution of policies regarding infrastructure, noting how policy has been influenced by experience—normal wear and tear, accidents, and natural hazards as well as terrorism. Readers will learn what fundamental attributes of infrastructure contribute to vulnerability, will be introduced to techniques for evaluating interdependence and vulnerability, and will learn about new developments in infrastructure technology that can reduce the consequences of terrorist attacks.

The Internet is a critical infrastructure that terrorists are unlikely to overlook as a potential target. Section 6 addresses problems of protecting cyberspace and offers a risk-management approach to cyberthreats. One chapter describes efforts by the federal government to assess risks and vulnerability in cyberspace; disseminate warnings; develop antiterrorist measures; coordinate the response to incidents; and provide technical assistance to organizations before, during, and after an incident. The chapter also offers guidelines for a robust information security program.

**Section 7: Border and Transportation Security**

This section covers security at borders, in immigration, in aviation, and in maritime settings—essential components of a nationwide counterterrorism strategy. “Porous” borders contributed to the defeat of the Soviet Union at the hands of the mujahideen in Afghanistan and as of this writing were enabling fighters to cross into Iraq to join the insurgents. Securing land, sea, and air borders—through which millions of people, planes, trucks, and containers pass annually—is a formidable challenge, especially if the necessary personnel are lacking.
Comparing civil aviation security in the United States before and after 9/11 can provide insight into the dynamics of homeland security. For example, the Transportation Security Administration (TSA) has given a high priority to screening baggage and passengers; but the rate of detection of explosives is still unsatisfactory, and airline cargo, shoulder-fired antiaircraft missiles, and other threats remain a concern.

In maritime security (as, typically, in homeland security in general), responsibility is fragmented among multiple agencies and the private sector. As a result, coordination and information sharing are crucial. The U.S. Coast Guard is the primary administrator of the Maritime Transportation Safety Act (MTSA), which one chapter in this section discusses in some detail.

This section also includes a case study of an envisioned statewide virtual network of transportation information to support decision making at all phases of homeland security.

Section 8: Emergency Management, Public Health, and Medical Preparedness

In the United States there is no national strategy to unify emergency management, public health, and medical preparedness. Here, a “system of systems” approach to risk management for homeland security is clearly needed. This approach must acknowledge the complexity of public health and the relationship among threats, vulnerabilities, and systems to understand specific weaknesses, allocate resources, and improve protection. In a large-scale emergency, it is necessary to move from a system of individual care to a system based on principles of public health and disaster management.

Section 8 provides an overview of the role of local first responders: emergency managers, firefighters, emergency medical personnel, and law enforcement officers. The Incident Command System (ICS) and the importance of reliable interoperable communications are discussed, as are the National Response Plan (NRP) and the National Incident Management System (NIMS). These are frameworks for managing and responding to domestic incidents that have “national significance,” such as terrorist threats, major disasters and emergencies, and catastrophic incidents.
One chapter takes up pre- and postattack mental health strategies, which are another crucial aspect of preparedness.

The section also includes a chapter about emergency management and preparedness procedures at hospitals in Israel. The authors share their experience treating casualties of suicide bombings and preparing for the effects of WMD.

**Section 9: Role of the Private Sector**

Public-private partnerships are crucially important in homeland security because, for one reason, the private sector owns or operates more than 85 percent of the nation’s critical infrastructure. This section provides practical advice for private-sector corporate security, risk and vulnerability assessment, emergency planning, crisis management, and planning. It includes an overview of the National Fire Protection Association (NFPA) standard on disaster and emergency management and business continuity programs.

One chapter in this section is a case study—a firsthand account of security measures taken by JW Marriott at its hotel in Jakarta—that provides an example of corporate crisis management in action. The section also covers two aspects of private-sector homeland security that are neglected by many companies. The first is the “human impact planning” to address the psychological health of employees and mitigate posttraumatic stress disorder; the second is legal issues that relate to homeland security and businesses, and measures that private industry can take to protect itself against liability in relation to a terrorist threat or incident.

**Section 10: Academe**

Academe played a vital role in determining how the Cold War would be fought. Now the academic sector must respond and restructure to meet new national security challenges. With regard to homeland security, academe can develop solutions through science and technology and can also offer education, training, outreach, and service. Academe is itself a potential target and resource for terrorists.

Homeland security is rapidly evolving as an academic course of study. One chapter in Section 10 suggests an interdisciplinary core curriculum for homeland security studies, to include such topics
as resource optimization and management, classic national security and international relations theory and practice, interfaces between technology and policy, organizational behavior, cultural understanding, strategic and scenario-based (futures) planning, and risk-based decision making. Operations research (OR) is an academic discipline that uses the scientific method to assess the consequences of alternative decisions involving long-term strategic planning and shorter-range tactics and operations. One chapter provides examples of how OR can be useful in emergency response plans and strategies, especially for first responders.

**Section 11: Science, Technology, and Information Sharing**

Inputs from many types of sensors, people, and software in homeland security produce a flood of information—and thus a challenge to “knowledge management.” Technology plays many roles in counterterrorist strategies for the private and public sectors. One role is combating chemical, biological, radiological, nuclear, and high-explosives (CBRNE) threats: for example, using systems to detect radiation at ports of entry. Technology also enables modeling, simulation, and analysis at each phase of emergency management. Data fusion, another tool of counterterrorism, gives decision makers and other public officials access to intelligence and analysis from the CIA, the FBI, and other government agencies.

Science and technology are particularly applicable in screening passengers and cargo for explosives—a capability that is essential for effective border and transportation security. However, many practitioners warn that simply “throwing technology” at a problem will not provide the desired security. One instance where this holds true is checkpoint security. Screening technologies must be integrated with a wider, holistic network, or security regime, within an organization, industry, region, or state and, ultimately, nationwide. Such integration requires wise technology policy and cooperation between the public and private sectors in order to result in increased efficiency and lower systemwide operational costs over the long term.

Many aspects of homeland security use information technology. One chapter in Section 11 explains why simply fusing data and information is unlikely to achieve the desired support for decision making. New IT “architecture” is needed to shift information sharing
from “need to know” to “need to share” in the face of cultural barriers. The section examines new IT concepts such as using computer systems with monitoring software and an array of sensors to identify a threat rapidly and provide a “predictive response.” One chapter presents a new paradigm for analyzing homeland security information-sharing needs by having distributed groups assess their needs collaboratively on an ongoing basis, using scenarios. This paradigm would constitute a key enabler for creating a broad-based information-sharing environment.

**Section 12: Domestic Security and Civil Liberties**

Security and liberty are both obligations of society. This section addresses various aspects of civil liberties in the context of homeland security. Topics include theoretical constructs and principles as well as actual and hypothetical examples. One chapter approaches the subject through three case studies (a proposed national identification card, bioterrorism, and the issue of racial and ethnic profiling). Data mining and surveillance raise special concerns about the invasion of privacy and are discussed in one chapter. These topics have become subjects of significant debate. Another chapter discusses the sensitive issue of balancing individual liberty and national security. When and where should free speech end in a post-9/11 world?

**Section 13: Politics and Accountability**

Homeland security gives rise to political questions that must be addressed—questions regarding values, principles, doctrine, the distribution of power, historic constitutional challenges, and accountability. All participants in homeland security must be accountable to the American people for a realistic set of performance measures. The three chapters in Section 13 address these issues and challenges.

David G. Kamien  
CEO, DGK LLC Homeland Security Management Consulting
INTRODUCTION

Homeland Security in Context

David Kamien
CEO, DGK LLC Homeland Security Management Consulting

The McGraw-Hill Handbook of Homeland Security explores both the threat of terrorism and the role of homeland security in dealing with this threat. This opening chapter surveys and contextualizes some of the key concepts and analytical frameworks used in the text.

HOMELAND SECURITY: KEY CONCEPTS

Homeland security is a policy framework for organizing the activities of government and all sectors of society to detect, deter, protect against, and, if necessary, respond to domestic attacks such as 9/11. Homeland Security is defined in the National Strategy for Homeland Security as “a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and recover from and minimize the damage of attacks that do occur” (Office of Homeland Security 2002, p. 2).

In the context of this National Strategy, prevention means action at home and abroad to deter, prevent, and eliminate terrorism. Vulnerability reduction means identifying and protecting critical infrastructure and key assets, detecting terrorist threats, and augmenting defenses, while balancing the benefits of mitigating risk against economic costs and infringements on individual liberty. Response and recovery means managing the consequences of attacks, and building and maintaining the financial, legal, and social systems to recover.

The National Strategy for Homeland Security categorized homeland security activities into six critical mission areas. The
White House Office of Management and Budget (OMB) 2003 Annual Report to Congress on Combating Terrorism described these missions as follows:

**Mission Area 1: Intelligence and Warning**

Terrorism depends on surprise. The first mission area includes intelligence programs and warning systems that can detect terrorist activity before it manifests itself in an attack so that proper preemptive, preventive, and protective action can be taken. Specifically, this mission area is made up of efforts to identify, collect, analyze, and distribute source intelligence information or the resultant warnings from intelligence analysis. As part of the homeland security category, this excludes funding for intelligence activities of the national security community that are focused overseas.

**Mission Area 2: Border and Transportation Security**

This second mission area includes border and transportation security programs designed to fully integrate homeland security measures into existing domestic transportation systems. Since current systems are intertwined with the global transport infrastructure, virtually every community in America is connected to the world by seaports, airports, highways, pipelines, railroads, and waterways that move people and goods into, within, and out of the nation. This mission area focuses on programs to promote the efficient and reliable flow of people, goods, and services across borders, while preventing terrorists from using transportation conveyances or systems as weapons, or to deliver implements of destruction.

**Mission Area 3: Domestic Counterterrorism**

The third mission area incorporates federal funding for any law enforcement programs (including state, local, or regional) that investigate and prosecute criminal activity to prevent and interdict terrorist activity within the United States. It includes all homeland security programs that identify, halt, prevent, and prosecute terrorists in the United States. It also includes pursuit not only of the individuals directly involved in terrorist activity but also of their
sources of support: the people and organizations that knowingly fund the terrorists and those that provide them with logistical assistance.

Mission Area 4: Protecting Critical Infrastructures and Key Assets

An attack on one or more pieces of our critical infrastructure could disrupt entire systems and cause significant damage. Programs that improve protection of the individual pieces and the interconnecting systems that make up our critical infrastructure belong in this fourth mission area. Programs associated with the physical security or cybersecurity of federal assets also belongs in this mission area. This area also includes programs designed to protect America’s key assets, which are those unique facilities, sites, and structures whose disruption or destruction could have significant consequences, including national monuments and icons.

Mission Area 5: Defending against Catastrophic Threats

The fifth mission area includes homeland security programs that involve protecting against, detecting, deterring, or mitigating terrorists’ use of weapons of mass destruction (WMD). It includes understanding terrorists’ efforts to gain access to the expertise, technology, and materials needed to build chemical, biological, radiological, and nuclear (CBRN) weapons. In addition, this mission area includes funding for planning and efforts to decontaminate buildings, facilities, or geographic areas after a catastrophic event.

Mission Area 6: Emergency Preparedness and Response

This sixth mission area includes programs that prepare to minimize the damage of and recover from any future terrorist attacks that may occur despite our best efforts at prevention. This area includes programs that help to plan, equip, train, and practice the needed skills of the various first-responder units, including such groups as police officers, firefighters, emergency medical providers, public works
personnel, and emergency management officials. This mission area also includes programs that will consolidate federal response plans and activities to build a national system for incident management in cooperation with state and local government.

The National Strategy describes four foundations for these six mission areas crossing all levels of government and sectors of society. These foundations are law, science and technology, information sharing and systems, and international cooperation. (See Figure I-3.)

Clearly these missions are all interrelated in many multidimensional ways. By imposing conceptual boundaries between these mission areas, one gains clarity for management and budgeting purposes. However, effective and viable plans and strategies can only be developed by acknowledging the complex reality that homeland efforts must cross mission areas, involve all levels of government and the private and public sectors, and coalesce into integrated, cross-cutting capabilities.

The last mission area—Emergency Preparedness and Response—merits special discussion, and is one area of homeland security where the notion of capabilities-based planning is being advanced. It also provides the context for discussing a macro-level tension in the field of homeland security. The December 2003 Gilmore Commission (formally known as the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction) report defines preparedness as "the measurable demonstrated capacity by communities, States, and private sector entities throughout the United States to respond to acute threats with well-planned, well-coordinated, and effective efforts by all of the essential participants, including elected officials, police, fire, medical, public health, emergency managers, intelligence, community organizations, the media, and the public at large" (Gilmore Commission 2003, p. 8).

The National Strategy for Homeland Security established a "National Vision for Emergency Preparedness and Response" that made emergency response for terrorist attacks, no matter how unlikely or catastrophic, as well as all manner of natural disasters, a national requirement. Homeland Security Presidential Directive 8 (HSPD-8) refers to preparedness for major events as "all-hazards preparedness." It defines major events as "domestic terrorist attacks, major disasters, and other emergencies." It presented a "National Preparedness Goal" to help achieve this vision of preparedness.
It defines *preparedness* as the “existence of plans, procedures, policies, training, and equipment necessary at the federal, state, and local level to maximize the ability to prevent, respond to, and recover from major events” (The White House 2003, p. 2). As a result, homeland security policy must manage a tension between preparing for terrorism per se and the broadly scoped “national preparedness” construct (for any major disaster or emergency event, including terrorist attacks, as part of “all-hazards” planning (e.g., planning for natural disasters).

That is not to say that the capabilities required to prepare for terrorism and other emergencies are wholly separate. The Office of Domestic Preparedness (ODP), Universal Task List (UTL) Manual (Version 1.0 draft of July 31, 2004) divides preparedness tasks into four levels: (1) national strategic tasks; (2) planning, coordination, and support tasks; (3) incident management tasks; and (4) incident prevention and response tasks, as follows:

1. National strategic (primarily federal departments and agencies)
   - Develop national strategic intelligence
   - Manage national preparedness activities
   - Conduct national prevention operations
   - Provide command and management of incidents of national significance
   - Provide national incident support
   - Manage national resources
   - Provide national communications and information management support
   - Develop supporting national technologies

2. Planning, coordination, and support (primarily single states or groups of states, regions within states or counties, federal regions)
   - Conduct intelligence operations
   - Conduct preparedness activities
   - Conduct prevention operations
   - Command and manage incidents of national or state significance
• Provide incident support
• Manage regional and state resources
• Provide communications and information management support

3. Incident management (mayor, city manager, county executive, or emergency operations center)

• Coordinate transportation operations
• Operate and/or manage telecommunications and information technology
• Manage and/or direct public works and engineering
• Coordinate firefighting operations
• Coordinate incident management operations
• Coordinate mass care, housing, and human services
• Coordinate resource support
• Coordinate public health and medical services
• Coordinate urban search and rescue
• Coordinate oil and hazardous materials response
• Coordinate agriculture and natural resource recovery
• Coordinate energy recovery
• Coordinate public safety and security
• Coordinate community recovery, mitigation, and economic stabilization
• Coordinate emergency public information and external communications

4. Incident Prevention and Response (incident site personnel)

• Provide transportation
• Operate telecommunications and information technology
• Conduct public works and engineering
• Conduct firefighting
• Conduct incident management
• Provide mass care, housing, and human services
• Provide resource support
• Provide public health and medical services
• Conduct urban search and rescue
Conduct oil and hazardous materials response
Support agriculture and natural resource recovery
Support energy recovery
Provide public safety and security
Support community recovery, mitigation, and economic stabilization
Provide emergency public information and external communications

Clearly terrorism-focused homeland security programs and broader all-hazards preparedness efforts require sets of capabilities that overlap to a significant degree. Still, in a world of limited time and financial resources, efforts made in a preparedness context or framework that tries to be too all-encompassing may run the risk of being ineffective.

HOMELAND SECURITY: A POLICY FRAMEWORK

The National Strategy for Homeland Security is one of a set of national strategies that interrelate. (See Figure I-1.)

Homeland security needs to be understood in the context of the broad spectrum of policy, frameworks, and instruments of national power for combating terrorism and national preparedness. According to the Office of Management and Budget (OMB), homeland security is a subset of “combating terrorism,” a policy framework that also includes “overseas combating terrorism” (OCT). Combating terrorism includes both antiterrorism (defensive measures used to combat terrorism) and counterterrorism (offensive measures used to combat terrorism), both domestically and abroad. (See Figure I-2.) Combating terrorism encompasses defense against WMD, improvements to critical infrastructure protection (CIP) to enhance the security of those physical and cyber-based systems essential to national security, national economic security, and public health and safety; and provision for federal “continuity of operations” (COOP)—those activities of federal agencies that ensure that the “mission-essential” functions of each agency continue no matter the cause of the disruption, even in the face of a catastrophic event.
Homeland security programs focus on activities within the United States and its territories, or on activities in support of domestically based systems and processes. The Homeland Security Council (HSC) coordinates these activities governmentwide. OCT includes activities that focus on combating and protecting against terrorism that occurs outside the United States and its territories. Such activities include efforts to detect, deter, protect against, and, if needed, respond to terrorist attacks. OCT does not include funding.
in support of the war on terrorism or other international conflicts. The National Security Council (NSC) coordinates these activities governmentwide. Together, the two areas account for the overall combating terrorism budget for the federal government.

Homeland security includes activities that focus on combating and protecting against terrorism that occur within the United States and its territories (this includes CIP and COOP), or outside the United States and its territories if they support domestically based systems or activities (e.g., prescreening high-risk cargo at overseas ports). Such activities include efforts to detect, deter, protect against, and, if necessary, respond to terrorist attacks.

**HOMELAND SECURITY MUST BE INTEGRATED WITH OVERSEAS POLICY FRAMEWORKS**

The center of gravity of homeland security is domestic and defensive. Yet terrorism is a transnational phenomenon, with roots and branches of recruiting, indoctrination, fund-raising, training, and attacking spread across the globe. Therefore, the counterterrorism “battle space” has “neither front lines nor geographic definition.” As the *Final Report of the 9/11 Commission* noted:

> In this sense, 9/11 has taught us that terrorism against American interests “over there” should be regarded just as we regard terrorism...
against America “over here.” In this same sense, the American homeland is the planet.¹

Because our society and economy are linked to and interdependent with the rest of the world, measures to defend the United States from threats such as a bomb in a cargo container extend internationally and depend on security efforts at foreign facilities. Many presumably domestic homeland security missions—border security and immigration, aviation and maritime security, intelligence, and law enforcement are some obvious examples—simply cannot be successful without international cooperation. Terrorists are finely attuned to differences in security regimes and will exploit seams between domestic and international counterterrorism.

Effective defensive measures influence a terrorist’s choice of targets or mode of attack but fail to deter terrorists who are smart, adaptive, and willing to undertake suicide attacks. Although homeland security does aim to prevent terrorists from reaching American soil and attacking, and domestic counterterrorism may succeed in apprehending terrorists in the United States, proactively confronting terrorists before they even attempt to reach the United States is preferable.

The National Strategy for Homeland Security is a subset of the National Strategy for Combating Terrorism, which emphasizes that all instruments of U.S. power are needed in combating international terrorism, both “at home” and “overseas.” In its final report the 9/11 Commission said:

The first phase of our post-9/11 efforts rightly included military action to topple the Taliban and pursue al Qaeda. This work continues. But long-term success demands the use of all elements of national power: diplomacy, intelligence, covert action, law enforcement, economic policy, foreign aid, public diplomacy, and homeland defense. If we favor one tool while neglecting others, we leave ourselves vulnerable and weaken our national effort (pp. 363–364).

Homeland security, as a policy instrument, mostly does not address the intricate root causes that give rise to terrorism in the first place and the broader context of dangerous global “chaos” described in this book. Only economic policy, foreign aid, various types of diplomacy and conflict resolution, education and time can affect the root causes of terrorism; and ultimately it is foreign governments and civilian communities, as well as the United States, that will
Figure I-3
Homeland security in context.

The Global Context:
- Terrorism
- Religious fanaticism
- Emerging infectious diseases
- WMD proliferation
- Failed states, lawless territories and massacres
- Organized crime and trafficking in people, drugs, arms, toxic substances, gems
- Piracy
- Cyberattacks

National Guidance Documents:
- Legislation and Congressional Oversight
- National Strategies
- Homeland Security Presidential Directives (HSPD)
- National Security Presidential Directives (NSPD)
- National Response Plan (NRP)
- National Incident Management System (NIMS)

Analytical Frameworks:
- Capabilities—based—planning
- Program performance assessment
- Strategic planning
  - Scenario-based planning
  - Mission area analysis
  - Universal task list
- Risk management

Results Management:
- Awareness
- Prevention
- Protection
- Response
- Recovery

Policy Tools for Combating Terrorism:
- Homeland security
- Homeland defense
- Military force
- Diplomacy
- Foreign aid
- Economic policy
- Law enforcement
- Intelligence
- Covert action

Political Context:
- Government organizational structure
- Funding
- Resource allocation
- Accountability
- Federalism
- Civil liberties (privacy, torture, speech)
- Role of military

National Strategy for Homeland Security:
- Intelligence and warning
- Border and transportation security
- Domestic counterterrorism
- Protecting critical infrastructures and key assets
- Defending against catastrophic threats
- Emergency preparedness and response

Figure courtesy of DGK LLC Homeland Security Management Consulting (www.kamien.com)
need to make hard decisions and take action in order to undermine support for terrorist ideology. Clearly, the success of overall counter-terrorism depends on internal and external integration of all national and international policy tools, strategies, and measures—including homeland security—into a carefully orchestrated global effort leaving no gaps in security that terrorists can exploit. (See Figure I-3.)

Whether or not the broader counterterrorism strategy is achieving its aims, delegitimizing terrorism and reducing the influence of the economic, political, religious, social, and psychological factors that motivate a person’s decision to use terror tactics is beyond the scope of this text. Regardless, it is unlikely that Islamist terrorists will cease to view the United States as an enemy anytime soon.

As long as the threat of terrorism and other disasters exists, as evidenced by the recent bombing in London, homeland security will remain relevant and important.

See also Chapter 16 Homeland Security’s National Strategic Position: Goals, Objectives, Measures Assessment and Chapter 18 The Department of Defense: Defending the Homeland and Defeating Enemies Abroad.

NOTES