

## Contents

### Preface *xiii*

<b>1</b>	<b>The Terrorist Threat</b>	<b>1</b>
1.1	What Is Terrorism?	1
1.2	The History of Terrorism	1
1.3	The Motivation for Terrorism	2
1.4	Can the Use of Terrorism be Justified?	3
1.5	The Role of Media in Terrorism	3
1.6	The Role of Social Media in Terrorism	4
1.7	Encryption	4
1.8	Civil Liberty and Terrorism	5
1.9	Terrorism Statistics	5
1.10	Purpose of Terrorism	8
1.11	Goals of Terrorism	8
1.12	Case Study: Economic Effects of a Terrorist Attack	9
1.13	Objectives of Terrorism	9
1.14	The Terrorism Challenge	10
1.15	The Evolution of Terrorism	10
1.16	Terrorist Tactics	10
1.17	Difference between Terrorism and Insurgency	10
1.18	The Difference between a Terrorist Attack, a Criminal Event, and Suspicious Activity	11
1.19	Case Study: Crime versus Terrorism	12
1.20	Common Terms in Terrorism	12
1.21	Types of Terrorist Organizations	14
1.22	International Terrorism	16
1.23	Examples of International Terrorist Groups	18
1.24	Recent International Terrorist Attacks	25
1.25	Domestic Terrorism	30
1.26	Examples of Domestic Terrorist Groups	32
1.27	Recent Domestic Terrorist Attacks	33
	References	35
	Questions	35
	Project	35
<b>2</b>	<b>Critical Infrastructure</b>	<b>37</b>
2.1	Introduction	37
2.2	Evolution of the Definition of Critical Infrastructure	37
2.3	Current Definition of Critical Infrastructure	40
2.4	Definition of Key Resources	41
2.5	Definition of Key Assets	41
2.6	Discussion of Critical Infrastructure	42
2.7	Soft Targets	49

2.8	Hard Targets	49
2.9	Cascading Effects from Interdependencies of Critical Infrastructures	50
2.10	Coordination of Critical Infrastructure Protection	51
2.11	Selection of Critical Infrastructure, Key Resources, and Key Assets	53
2.12	Identification and Selection of Soft Targets by a Jurisdiction	54
2.13	Target Attractiveness	54
2.14	Inventorying and Prioritizing Critical Infrastructure/Key Resources/Key Assets/ Soft Targets	55
	References	64
	Questions	65
	Project	65
	Appendix 2.1 Executive Order 13010 by President William J. Clinton	65
	Appendix 2.2 Presidential Decision Directive 63 by President William J. Clinton	67
	Annex A: Structure and Organization	71
	Annex B: Additional Taskings	73
	Appendix 2.3 Executive Order 13228 by President George W. Bush	75
	Appendix 2.4 Executive Order 13231 by President George W. Bush	79
	Appendix 2.5 Homeland Security Presidential Directive 7 by President George W. Bush	85
	Appendix 2.6 Presidential Policy Directive 21 by President Barack Obama	90
<b>3</b>	<b>Types of Terrorist Attacks</b>	<b>99</b>
3.1	Introduction	99
3.2	Types of Destructive Events	99
3.3	Who Can Execute an Attack?	100
3.4	Ways in Which a Critical Asset May Be Attacked	101
3.5	Target Selection	103
3.6	Identifying Lucrative Targets	104
3.7	Characteristics of a Terrorist Attack	106
3.8	Results of a Successful Terrorist Attack	106
3.9	Terrorist Tactics	107
3.10	Case Study of a Terrorist Attack	119
3.11	The Interrupted Terrorist Plots	120
	References	120
	Questions	121
	Project	121
	Appendix 3.1 Executive Order 13636 by President Barack Obama Executive Order 13636 of February 12, 2013	121
	Appendix 3.2 Presidential Policy Directive 21 by President Barack Obama	126
	Appendix 3.3 Presidential Policy Directive 41 by Barack Obama	133
<b>4</b>	<b>Weapons of Mass Destruction</b>	<b>137</b>
4.1	Introduction	137
4.2	History of Weapons of Mass Destruction	138
4.3	Why Use a Weapon of Mass Destruction?	139
4.4	Limitations of the Use of Weapon of Mass Destruction Materials	139
4.5	Indicators of a Possible Weapon of Mass Destruction Attack	140
4.6	Results of a Weapon of Mass Destruction Attack	140
4.7	How a Chemical, Biological, or Radiological Agent Can Enter the Body	140
4.8	Effectiveness of a Chemical, Biological, or Radiological Attack	141
4.9	Obtaining a Weapon of Mass Destruction	142
4.10	Questions about Weapons of Mass Destruction	142
4.11	Types of Weapons of Mass Destruction	143
4.12	Other Weapons Used by Terrorists	178
4.13	Weaponization of Chemical and Biological Agents	179
	References	184



	Questions	184
	Project	185
<b>5</b>	<b>The Terrorist's Preparation for an Attack</b>	<b>187</b>
5.1	General	187
5.2	Target Considerations	187
5.3	The Terrorist's Investment	187
5.4	Example of Terrorist Financing	188
5.5	Eight Indicators of Terrorism	189
5.6	Raising Suspicion	200
5.7	Summary of Attack Process	200
	References	201
	Questions	201
	Project	201
<b>6</b>	<b>Risk and Threat Assessment</b>	<b>203</b>
6.1	Introduction	203
6.2	Definitions	203
6.3	The Risk of Attack	203
6.4	Risk	204
6.5	Risk Management	212
6.6	Risk Assessment and Management Approach	216
6.7	Probability of Attack Occurrence	221
6.8	Consequences of a Successful Attack	222
6.9	The CARVER Assessment Tool	222
6.10	Threat and Hazard Identification and Risk Assessment Guide (THIRA)	225
	References	233
	Questions	233
	Project	233
	Appendix 6.1 Presidential Policy Directive 8 by President Barack Obama	233
<b>7</b>	<b>The Security Vulnerability Analysis</b>	<b>237</b>
7.1	Introduction	237
7.2	What is a Security Vulnerability Analysis?	237
7.3	The Purpose of a Security Vulnerability Analysis	238
7.4	Preparing to Conduct a Security Vulnerability Analysis	240
7.5	The Security Vulnerability Analysis Process	240
7.6	Administrative Functions in the Security Vulnerability Analysis Process	246
7.7	Risk Assessment	248
7.8	Preparing to Conduct a Threat and Risk Analysis	249
7.9	The Buffer Zone Protection Plan	254
7.10	The CARVER Target Analysis Tool	255
	Reference	257
	Questions	257
	Project	257
<b>8</b>	<b>Principles of Protective Security</b>	<b>259</b>
8.1	Introduction	259
8.2	Prevention	259
8.3	Information Collection	260
8.4	Information Sharing	260
8.5	Risk Mitigation	262
8.6	Cost-Benefit Analysis	262
8.7	Situational Awareness	263

8.8	Security	264
8.9	Suspicious Activity	268
8.10	What Can Be Done to Protect People and Facilities	270
8.11	Conclusion	277
8.12	References	278
	Questions	278
	Project	278
<b>9</b>	<b>Effective Security Countermeasures</b>	<b>279</b>
9.1	Introduction	279
9.2	Counterterrorism Policy: National Security Strategy	279
9.3	Hardening and Strengthening	280
9.4	What Are Security Countermeasures?	281
9.5	Management of Change	285
9.6	Risk Management	285
9.7	Critical Asset Resiliency	285
9.8	Critical Infrastructure Protection	288
9.9	Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks	289
9.10	All Hazards Protection	291
9.11	Cost-Benefit Analysis	291
9.12	Information Sharing and Analysis Centers	291
9.13	Private Sector's Responsibility	291
9.14	Protecting Critical Infrastructure, Key Resources, and Key Assets	292
9.15	Standoff Distance	303
9.16	Response to an Active Shooter	303
9.17	Preparing for Attacks on Transportation	306
9.18	Administrative Security Enhancements	306
9.19	Recommendations for Enhanced Security Through Various ISACs	320
	References	326
	Questions	327
	Project	327
	Appendix 9.1 Directive on National Continuity Policy, NSPD 51/HSPD 20, by President George W. Bush	327
	Appendix 9.2 Homeland Security Presidential Directive 8 by President George W. Bush	331
<b>10</b>	<b>General Emergency Response Considerations</b>	<b>335</b>
10.1	Introduction	335
10.2	Definition of First Responder	335
10.3	Emergency Response Plans	335
10.4	Pre-incident Planning	337
10.5	Drills and Exercises	338
10.6	Emergency Response Priorities	341
10.7	Operational Risk Management	342
10.8	Situational Awareness	344
10.9	Homeland Security Presidential Directive 5	344
10.10	The Incident Command System	347
10.11	Determining Potential Outcomes	353
10.12	Approving the Level of Personal Protective Equipment	354
10.13	Developing a Plan of Action	356
10.14	Components of the Incident Command System	359
10.15	Media Relations	366
10.16	Evaluating Progress of the Plan of Action	368
10.17	Terminating the Incident	368
10.18	Critical Incident Stress	370
10.19	Family Preparedness	371



References	371
Questions	271
Project	271
Appendix 10.1 Homeland Security Presidential Directive 5 by President George W. Bush	372
Appendix 10.2 Incident Command System Form 208	376
<b>11 Emergency Response to a Weapon of Mass Destruction Attack</b>	<b>379</b>
11.1 Introduction	379
11.2 Use of a Weapon of Mass Destruction	379
11.3 The Emergency Scene as a Crime Scene	379
11.4 Size Up	381
11.5 The Secondary Device	381
11.6 Evacuation of Personnel in a Weapon of Mass Destruction Attack	382
11.7 Protecting Building Environments from Airborne Agents	384
11.8 Emergency Response Actions at the Scene of a Weapon of Mass Destruction Incident	384
References	411
Questions	411
Project	411
<b>12 Homeland Security Laws, Regulations, and Standards</b>	<b>413</b>
12.1 What Is Homeland Security?	413
12.2 2002 National Strategy for Homeland Security	413
12.3 The 2007 National Strategy for Homeland Security	421
12.4 Office of Homeland Security	423
12.5 The Department of Homeland Security	423
12.6 The Transportation Security Administration	426
12.7 The Chemical Facility Anti-Terrorism Standards	427
12.8 The Chemical Facility Anti-Terrorism Standards of 2014	428
12.9 Chemical Terrorism Vulnerability Information	428
12.10 CVI Authorized User Training	430
12.11 Protected Critical Infrastructure Information Program	430
12.12 Chemical Security Assessment Tool	432
12.13 CFATS Top Screen	432
12.14 Enhanced CFATS Tiering Methodology	433
12.15 Security Vulnerability Assessment	435
12.16 Site Security Plan/Alternative Security Plan	435
12.17 CFATS Facility Inspections	437
12.18 CFATS Ongoing Compliance	438
12.19 Regional Resiliency Assessment Program	438
12.20 Maritime Transportation Security Act	439
12.21 US Coast Guard Maritime Security Levels	443
12.22 Transportation Worker Identification Credential	444
References	444
Questions	445
Project	445
Appendix 12.1 Authorizing Statute for the Chemical Facility Anti-terrorism Standards Regulations (6 CFR Part 27)	445
Appendix 12.2 CFATS Appendix A, List of COI, and STQ	447
Appendix 12.3 CFATS Act of 2014	463
Appendix 12.4 US Coast Guard Facility Vulnerability and Security Measures Summary	477
<b>Index</b>	<b>481</b>