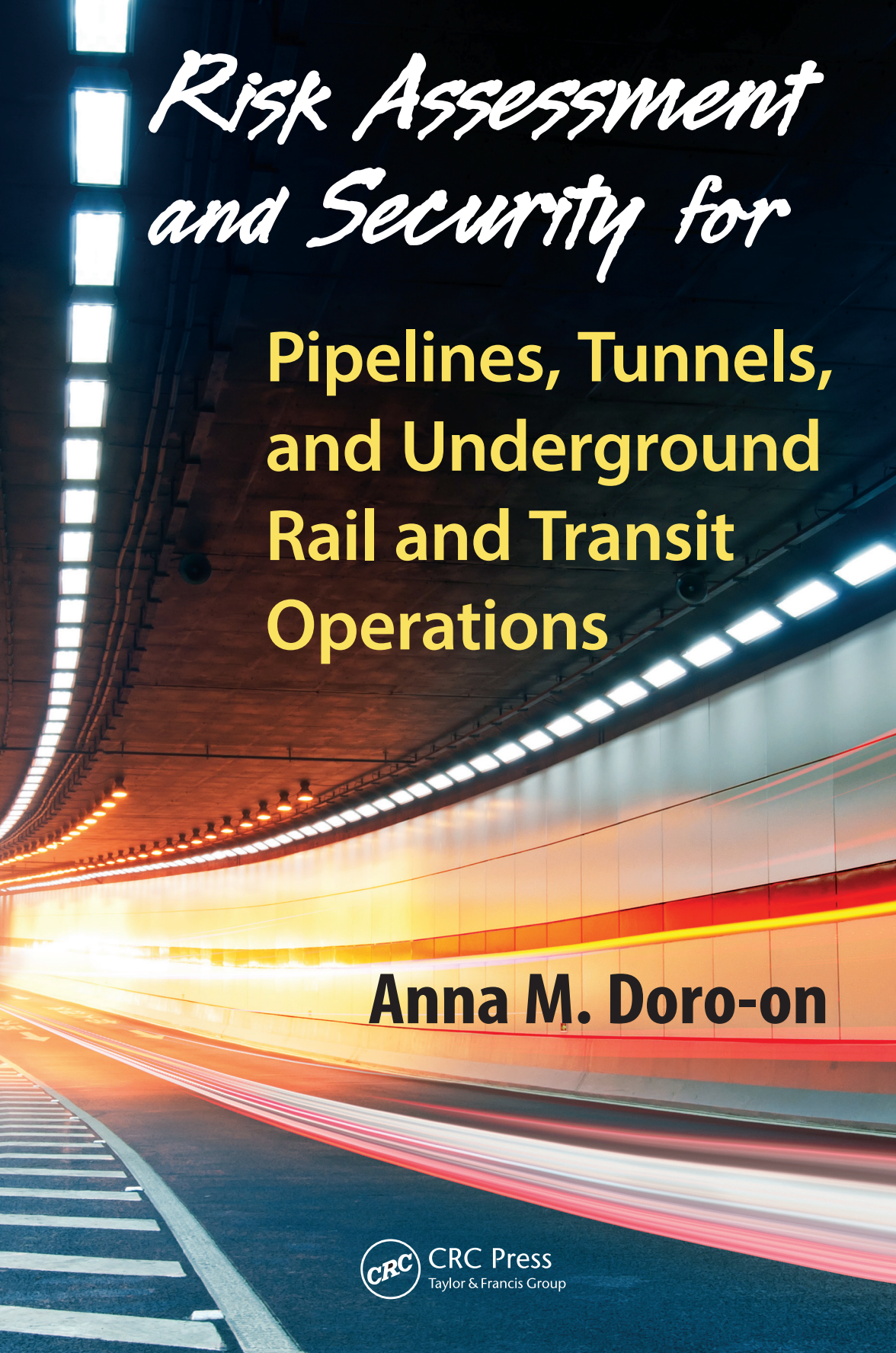

Risk Assessment and Security for
Pipelines, Tunnels, and Underground Rail and Transit Operations
Anna M. Doro-on
CRC Press
Taylor & Francis Group

Risk Assessment and Security for

Pipelines, Tunnels, and Underground Rail and Transit Operations

Risk Assessment and Security for

Pipelines, Tunnels, and Underground Rail and Transit Operations

Anna M. Doro-on

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2014 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20130923

International Standard Book Number-13: 978-1-4665-6934-8 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

I dedicate this book to my fellow citizens, heroes, warfighters, and to those who continually work so hard to protect our nation and allies,

and in memory of my little brother, Romwel, who passed away on June 22, 2013. I could not have done this work without all of you.

—

Uncertainty dwells when knowledge and wisdom regarding past and future events are absent. Death brings with it final certainty.

Thought without discernment leads to flawed decisions,
Judgment based on gut feeling is an alley to incongruous choice,
Unsound decision leads to a dangerous abyss.

Information detects the smoking motions of the enemy,
Imagination destroys the raging fires,
Thus, information and imagination are the most powerful weapons of all.

Heroes protect and defend American hopes and dreams,
Their mission is to shield us with indestructible armors and weapons,
And they live, survive—they never die.

Oh Mother Nature! We want you to be happy and
willingly join the battle to defend our freedom!

—

I dedicate this book to my mentors who supported my endeavors:

Robert Linza, John Weatherford, Mark Listewnik, Rocky Shih, and Timothy Brotherton.

To my parents Arch. Marcela and Engr. Romeo Doro-on for the talent that I inherited from them. To my younger brothers Romwel and Romcel and to Anna Liza, Rommel, and Auntie Fe Nolte for keeping me strong with their guidance and endless love.

Contents

Preface ..... **xix**
Acknowledgments ..... **xxi**
Author ..... **xxiii**

1 Introduction **1**
1.1 Background 1
1.2 Risk Acceptability of Terrorism and Disaster 2
1.3 Objective 2
1.4 Scope 2
1.5 Purpose 3

2 Hazards, Terrorism, and Weapons of Mass Destruction on Pipelines, Tunnels, and Underground Rail and Transit Systems **5**
2.1 Introduction 5
2.1.1 Terrorism and Disasters against Pipelines, Tunnels, Underground Rail, and Transit Systems 6
2.2 Understanding the Basic Structure of Terror Organization 6
2.2.1 Basic Recruitment Operations 6
2.2.2 Terror Aspirant and Self-Radicalization 6
2.2.3 Terror Member 7
2.2.4 Terror-Suicide Bomber 7
2.2.5 Technical Bomb and Improvised Explosive Devices Developer 7
2.2.6 Terrorists Specializing in Chemical Threat 7
2.2.7 Terrorists Specializing in Biological Threat 8
2.2.8 Terrorists Specializing in Radiological and Nuclear Weapons 8
2.2.9 Terrorist Intelligence Information and Reconnaissance Operation 8
2.2.10 Terror Planner and Military Operation Planner 8

2.3 Weapons of Mass Destruction 8
2.4 Chemical Explosives 10
2.4.1 Acetone Peroxide 11
2.4.2 Ammonium Nitrate 12
2.4.3 Ammonium Nitrate–Fuel Oil 13
2.4.4 Cyclonite (RDX) 13
2.4.5 Dingu and Sorguyl 14
2.4.6 Hexamethylenetetramine Dinitrate 14
2.4.7 Hexanitroazobenzene 14
2.4.8 Hexanitrodiphenylamine 15
2.4.9 Hexanitrohexaazalsowurtzitane 16
2.4.10 Lead Azide 18
2.4.11 Lead Styphnate 19
2.4.12 Mercury(II) Fulminate 20
2.4.13 Nitrocellulose 22
2.4.14 Nitroglycerin 24
2.4.15 Octagen (HMX) 24
2.4.16 Pentaerythritol Tetranitrate 24
2.4.17 Picric Acid 26
2.4.18 Plastic Explosives 26
2.4.19 2,4,6-Trinitrotoluene 28
2.5 Mechanical Components and Applications of Chemical Explosives 31
2.5.1 Alginates 32
2.5.2 Aluminum Powder 32
2.5.3 Base Charge 32
2.5.4 Blasting Caps 32
2.5.5 Blasting Galvanometer 32
2.5.6 Blasting Machine 32
2.5.7 Blast Meters and Boosters 33
2.5.8 Bridgewire Detonator 33
2.5.9 Brisance 33
2.5.10 Deflagration 34
2.5.11 Delay Time and Element 34
2.5.12 Detonation 34
2.5.12.1 Shock Wave 34
2.5.12.2 Detonation Wave Theory 36
2.5.12.3 Selective Detonation 37
2.5.12.4 Sympathetic Detonation 37
2.5.12.5 Detonation Development Distance 38
2.5.13 Electroexplosive Device 38
2.5.14 Oxidizer and Oxygen Balance of Explosives 38

2.5.15 Heat of Explosion 38
2.5.16 Underwater Detonation 38
2.5.16.1 Shock Wave of Underwater Detonation 39
2.5.16.2 Gas Bubble 39
2.5.17 Calculation of Explosives 40
2.5.18 Hazards of Explosives 40
2.6 Chemical Threats as Poisonous Weapons and Lethal Dose (LD_{50}) 40
2.6.1 Chemicals' LD_{50} 45
2.6.2 Cyanide 46
2.6.2.1 Cyanide LD_{50} 46
2.6.3 Mustard Agents 46
2.6.4 Nerve Agents 47
2.6.5 Toxic Industrial Agents 47
2.6.6 Arsenic 47
2.6.6.1 Arsenic LD_{50} 48
2.6.7 Inorganic Contaminants 48
2.6.8 Organic Contaminants 51
2.7 Biological Weapons 51
2.8 Radiological and Nuclear Threats 51
2.8.1 Radiological Dispersion Device 53
2.8.2 Improvised Nuclear Device 53
2.8.3 Nuclear Reactor Accident 53
2.8.4 Nuclear Weapon 53
2.9 Natural Disaster and Hazard 60
2.9.1 Earthquakes 64
2.9.2 Extreme Heat 66
2.9.3 Floods 71
2.9.4 Hurricanes 75
2.9.5 Landslides and Mudslides 75
2.9.6 Tornadoes 76
2.9.7 Tsunamis 76
2.9.8 Volcanoes 76
2.9.9 Wildfires 77
2.9.10 Winter Weather 78
2.9.11 Lightning 78
2.9.12 Avalanches 78
2.9.13 Ultraviolet 79
2.9.14 Space Weather 79
2.10 Cyberterrorism 80
2.11 Implications 81
References 81

3 Introduction to Pipelines, Tunnels, Underground Rail and Transit Operations, Terrorism, and Disasters 89
3.1 Introduction 89
3.2 Disaster and Acts of Terrorism against Pipelines, Tunnels, and Underground Rail and Transit Systems 90
3.2.1 Security for Hazardous and Radioactive Material Transport Systems 91
3.2.2 Fire, Explosion, and Detonation 93
3.2.2.1 Vapor Cloud Explosion and Jet Flames 95
3.2.2.2 Flash Point 95
3.2.2.3 Flammability Range 95
3.2.2.4 Autoignition Temperature 95
3.2.2.5 Flame Speed and Burning Velocity 96
3.2.2.6 Pool Fires 96
3.2.3 Emission and Dispersion 98
3.2.3.1 Dispersion Situation: Buoyancy Effects 100
3.2.3.2 Dispersion Situation: Momentum Effects 101
3.2.3.3 Dispersion Situation: Source Terms 101
3.2.3.4 Dispersion Situation: Source Elevation 101
3.2.3.5 Dispersion Situation: Meteorology and Topography 101
3.2.3.6 Dispersion Situation: Building and Obstructions 101
3.2.4 High Toxic Release 101
3.2.5 Dust and Fragment Explosion 102
3.2.5.1 Explosion Process 102
3.2.6 Freight Capsule or Vessel Burst Pressure and Energy Distribution 103
3.2.7 Explosion Destruction by Missiles 103
3.2.7.1 Sources, Types, and Propagation of Missiles 103
3.2.7.2 Number and Size of Missiles 103
3.2.7.3 Velocity of Missiles 103
3.2.7.4 Angle of Departure of Missiles 104
3.2.7.5 Shape, Air Resistance, and Flight of Missiles 104
3.2.7.6 Flying Glass 104
3.2.7.7 Falling Masonry and Glass 105
3.3 Underground Freight Transportation through Pipelines, Tubular Rail, and Magnetic Levitation 105
3.3.1 Automated Transportation System 105
3.3.2 Automated Transportation Logistic System 105
3.3.3 Underground Transportation Logistic System 106
3.3.4 Pneumatic Capsule Pipeline for Underground Freight 106

3.3.5 CargoCap 106
3.3.6 Underground Container and Capsule Transport Systems 107
3.3.7 Tubular Rail 109
3.3.8 Magnetic Levitation Transportation System 109
3.4 Railroad and Railway Systems 110
3.5 Oil, Gas, and Other Hazardous Liquid Pipelines 112
3.5.1 Unregulated Hazardous Material Liquid Pipelines 113
3.6 Underwater/Immersed Tunnel and Cross-River Tunnel 114
3.7 Transportation Tunnels 116
3.7.1 Road Tunnels 116
3.7.2 Transit and Rail Tunnels 117
3.8 Mine Tunnels 118
3.9 Drainage Tunnels 119
3.10 Aqueducts 119
3.11 Defense and Warfare Tunnels 119
3.12 Illegal Underground Tunnels 121
3.13 Implication 122
References 122

4 Risk and Vulnerability Assessment 131
4.1 Introduction 131
4.2 National Aeronautics and Space Administration Risk Analysis and Management 131
4.2.1 Risk Matrices 132
4.2.2 FMECAs, FMEAs, and Fault Trees 133
4.2.3 NASA Probabilistic Risk Assessment 133
4.3 Standard Homeland Security Risk Assessment and RAMCAP Plus Processes 134
4.3.1 Fatalities and Serious Injuries 137
4.3.2 Financial and Economic Impacts 137
4.3.3 Vulnerability Analysis 147
4.3.4 Threat Assessment 147
4.3.5 Risk and Resilience Assessment 149
4.3.6 Risk and Resilience Management 150
4.4 Department of Defense Risk Assessment and Management 150
4.4.1 Risk Reporting Matrix 151
4.4.2 Security Risk Categories 154
4.5 CARVER Matrix 157
4.5.1 Criticality 158
4.5.2 Accessibility 158
4.5.3 Recuperability 159

4.5.4 Vulnerability....160
4.5.5 Effect....161
4.5.6 Recognizability....161
4.6 CARVER + Shock....162
4.7 Model-Based Vulnerability Analysis....162
4.8 Freight Assessment System....165
4.9 Federal Emergency Management Agency HAZUS-MH....166
4.10 Security Vulnerability Assessment....167
4.11 Automated Targeting System....169
4.11.1 ATS-Inbound....171
4.11.2 ATS-Outbound....172
4.11.3 ATS-Passenger....172
4.11.4 ATS-Land....172
4.11.5 ATS-International....172
4.11.6 ATS-Trend Analysis and Analytical Selectivity....172
4.12 Sandia National Laboratories Security Risk Assessment Methods....172
4.13 ASME RA-S Probabilistic Risk Assessment....173
4.14 Development of Prospect Theory....174
4.14.1 Expected Utility Theory....175
4.14.2 Prospect Theory....175
4.15 Cumulative Prospect Theory....175
4.15.1 Framing Effects....175
4.15.2 Nonlinear Preferences....175
4.15.3 Source Dependence....176
4.15.4 Risk Seeking....176
4.15.5 Loss Aversion....176
4.15.6 Cumulative Prospect Theory....176
4.16 Conclusion....178
References....178

5 Quantitative Risk Estimation Model for Pipelines, Tunnels, Underground Rapid Rail, and Transit Systems....181
5.1 Introduction....181
5.2 Elements of Risk Assessment....182
5.2.1 Risk Estimation Development for Terrorism against Pipelines, Rails, and Tunnels....182
5.2.2 Risk Estimation Development for Clandestine Fabrication and Transshipment of Weapons of Mass Destruction by Terrorists and Rebellious States to Endangering Homeland Security....183
5.3 Event Tree Analysis....184
5.4 Estimation of Risk and Risk Factors....190

5.4.1 Calculation of Risk Rate 191
5.4.2 Life Expectancy Models 195
5.5 Fault Tree Analysis 197
5.5.1 Example of Event Tree Analysis 197
5.6 Identification of Hazards 200
5.7 Terrorism Intrusion 201
5.8 Flash Fire Probability 201
5.9 Flash Fire: Ignition of Flammable Materials 201
5.10 Detonation of Explosive Devices 204
5.11 Large-Scale WMD Detonation 210
5.12 Pipelines, Tunnels, Underground Rail, and Transit Systems Adjacent to Human Population 210
5.13 Guideway Short Circuit 210
5.14 Pipelines, Tunnels, Underground Rail, and Transit Systems Adjacent to Critical Assets 211
5.15 Pipelines, Tunnels, Underground Rail, and Transit System Rupture 211
5.16 Sensor Failure 211
5.17 Mechanical and Electrical Failure 211
5.18 Capsules, Underground Rail, and Transit System Derailment and Collision 211
5.19 HAZMAT Freight Container and Pipeline Damage, Collapse, and Spill 212
5.20 Risk Index Matrix 212
5.21 Human Injury Risk 212
5.22 Implication 213
References 213

6 Risk Acceptability Analysis Based on Quantitative Psychology of Intuitive Judgments 215
6.1 Introduction 215
6.1.1 Public Perception of Risk: Quantitative Psychology of Intuitive Judgment and Cumulative Prospect Theory 216
6.1.1.1 Voluntary or Involuntary 221
6.1.1.2 Discounting Time 222
6.1.1.3 Identifiability of Taking a Statistical Risk 222
6.1.1.4 Controllability 222
6.1.1.5 Avoidability of Risks 223
6.1.1.6 Position in Hierarchy of Consequence 223
6.1.1.7 Ordinary or Catastrophic 223
6.1.1.8 Natural or Man-Originated 224
6.1.1.9 Magnitude of Probability of Occurrence 224

6.2 Strategic Determination of Risk Acceptability....225
6.3 Quantitative Revealed Societal Preference Method 225
6.3.1 Behavior and Risk Attitude 228
6.3.2 Establishing Risk Comparison Factors 228
6.3.3 Controllability of Risks 228
6.3.4 Perceived Degree of Control....229
6.3.5 System Control in Risk Reduction 229
6.3.5.1 Systemic Control of Risk....229
6.3.5.2 Control Factors....232
6.3.6 Controllability of New Technological Systems 232
6.3.7 Cost–Benefit Analysis....232
6.3.8 Prerequisites for Risk Acceptance of Terrorist Attacks and Disaster.... 234
6.3.8.1 Requirement for a Methodology.... 234
6.4 Establishing the Risk Referent....236
6.4.1 Multiple Risk Referents....236
6.4.2 Risk Proportionality Factor Derivation from Risk References....237
6.4.3 Risk Proportionality Derating Factors....238
6.4.4 Degree of Systemic Control....238
6.4.5 Conversion of a Risk Reference to a Risk Referent 240
6.5 Implication....241
References....241

7 Strategic Intelligence Analysis, Military Support, and Military Intuitive Judgment in Safeguarding Pipelines, Tunnels, Underground Rail and Transit Operations, and Homeland 245
7.1 Introduction....245
7.2 Intelligence Analysis.... 246
7.3 Standard Intelligence Analysis Cycle 249
7.4 Quantitative Risk Estimation for the Intelligence Analysis of Infrastructure Protection and WMD Mitigation....252
7.5 Intelligence Analysis Development: Risk Estimation Models for Rail System Threat and Intuitive Predictions for the Smuggle of WMD Components and Clandestine Terror-Military Operations 252
7.6 Intelligence Analysis: Event Tree Analysis Model 256
7.7 Perspectives of Risk Acceptability in Strategic Intelligence Analysis.... 264
7.7.1 Risk Estimation and Risk Acceptability 270
7.8 Perspectives of Risk Acceptability Analysis for Pipelines, Tunnels, Underground Rail, and Transit Systems....270
7.9 Military Intuitive Judgment and Decision-Making Process....288

7.9.1 Command of the Armed Forces and the Chain of Command 306
7.9.2 Understanding Military Operations 309
7.10 Requirement of Military Support for Critical Infrastructure and Homeland Security 310
7.10.1 Intelligence 311
7.10.2 Northern Command 312
7.10.3 Department of Defense: Chemical, Biological, Radiological, and Nuclear Incident Response 313
7.10.3.1 US Army Chemical Material Agency 315
7.10.3.2 US Army Research, Development, and Engineering Command 315
7.10.3.3 US Army—20th Support Command Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Analytical Remediation Activity 315
7.10.3.4 US Army—20th Support Command Chemical, Biological, Radiological, Nuclear, and Explosives 315
7.10.3.5 Joint Program Executive Office for Chemical and Biological Defense 316
7.10.3.6 National Guard Weapons of Mass Destruction: Civil Support Teams 316
7.10.3.7 US Army Special Operations Command 317
7.10.4 Posse Comitatus Act: USC Title 18, §1385 317
7.10.5 Insurrection Act: USC Title 10, §331–335, Chapter 15 318
7.10.6 Military Support to Civilian Authorities: USC Title 10, §371–382, Chapter 18 319
7.10.7 Military Support: Maintenance of Other Troops: USC Title 32, §109, Chapter 1 319
7.10.8 National Guard for Homeland Defense Duty: USC Title 32, §904, Chapter 9 320
7.10.9 Response to Threats of Terrorist Use of Weapons of Mass Destruction: USC Title 50, §2311, Chapter 40 321
7.10.10 Presidential Policy Directive 8 321
7.10.11 Manual for Civil Emergencies: DoD3025.1M 323
7.10.12 Military Support to Civilian Authorities: DoDD 3025.1 323
7.10.13 Military Assistance to Civilian Authorities: DoDD 3025.15 324
7.11 Implication 324
References 326

8 Preparedness, Preventive, and Defensive Measures 331
8.1 Introduction 331
8.2 National Response Framework 332
8.2.1 Local Governments 333
8.2.1.1 Roles of Chief Elected or Appointed Officials 333
8.2.1.2 Roles of Emergency Managers 333
8.2.1.3 Roles of Department and Agency Heads 333
8.2.1.4 Roles of Individuals and Households 333
8.2.2 States, Territories, and Tribal Governments 334
8.2.2.1 Roles of the Governor 334
8.2.2.2 Roles of the State Homeland Security Adviser 334
8.2.2.3 Roles of the Director of the State Emergency Management Agency 335
8.2.2.4 Roles of Other State Departments and Agencies 335
8.2.2.5 Roles of Indian Tribes 335
8.2.2.6 Roles of Tribal Leaders 335
8.2.3 Federal Government 335
8.2.3.1 Role of the Secretary of Homeland Security 336
8.2.3.2 Law Enforcement 336
8.2.3.3 National Defense and Defense Support of Civil Authorities 336
8.2.3.4 International Coordination 336
8.2.3.5 Intelligence 336
8.2.3.6 Private Sector and Nongovernmental Organizations 337
8.2.3.7 Roles of Private Sector 337
8.2.3.8 Roles of Nongovernmental Organizations 337
8.2.3.9 Roles of Volunteers and Donors 337
8.3 Emergency Preparedness 337
8.3.1 Planning 337
8.3.2 Organization 338
8.3.3 Equipment 338
8.3.4 Training 338
8.3.5 Exercises, Evaluation, and Improvement 338
8.4 Response 339
8.4.1 Baseline Priorities 339
8.4.2 Local, Tribal, and State Actions 339
8.4.3 Federal Actions 340
8.4.4 Alerts 340
8.4.5 Operations Center 340
8.5 Activate and Deploy Resources 340

8.6 Proactive Response to Catastrophic Incidents....341
8.7 Recovery....341
8.8 Preventive and Defensive Measures....341
8.8.1 Oil and Gas Pipeline Protection....341
8.8.2 Road, Highway, and Rail Tunnel Protection....342
8.8.2.1 Fire and Emergency Response....342
8.8.2.2 Preventive Systems for Road and Highway Tunnels....343
8.8.2.3 Preventive Measures for Terrorism....345
8.8.2.4 Minimum Standard Preventive Measures....347
8.8.2.5 High Standard Preventive Measures....349
8.8.3 System Protection Interoperability for Road, Highway, and Rail Tunnels....351
8.8.3.1 Emergency Responders and Operating Procedures....351
8.8.4 Engineering and Salient Features of Technological Systems....352
8.9 Mine Tunnels Hazard Prevention....352
8.9.1 Lighting in Mine Tunnels....352
8.9.2 Emergency Supply Facilities....353
8.9.3 Thermal Stress....353
8.9.4 Access....353
8.9.5 Well-Being Monitoring....353
8.9.6 Training....354
8.9.7 Personal Safety Devices and Accessories....354
8.9.8 Surface Area Boundary Planning and Design....354
8.9.9 Hazard, Vulnerability, and Risk Management of Mine Tunnels....355
8.9.10 Hazardous Substances....356
8.9.11 Fire and Explosion....356
8.9.12 Heating and Inundation....356
8.9.13 Outburst and Rockburst....357
8.9.14 Strata Control in Mine Tunnels....357
8.9.15 Mine Tunnel Explosive Materials Handling....358
8.9.16 Mine Tunnel Ventilation....358
8.9.17 Mine Tunnel Ventilation System Planning....359
8.9.18 Airways, Air Crossings, and Stoppings....359
8.9.19 Mine Tunnel Emergency Response: Fire Control and General Emergency Systems....359
8.10 Approaches for the Detection of Illegal Tunnels by Other Experts....360
8.10.1 Ground-Penetrating Radar....362

8.10.2 Seismic Waves 362
8.10.3 Electrical Resistivity 362
8.10.4 Microgravity and Gravity Surveying 362
8.10.5 Cosmic Rays....363
8.10.6 Cross-Well Radar....363
8.10.7 High-Resolution Seismic Methods 363
8.10.8 Approach to the Tunnel Detection Agent-Based Model 364
8.10.9 Electromagnetic Induction 365
8.10.10 Tunnel Detection Using Forward Scatter between Borehole Signal Sources....365
8.10.11 Fiber-Based Brillouin Optical Time Domain Reflectometry 365
8.11 Approaches for the Detection of Land Mines and Improvised Explosive Devices by Other Experts 366
8.11.1 Weapons Technological Intelligence....367
8.11.2 Ultra-Wideband Microwave Technology 368
8.11.3 Foot Patrols 368
8.11.4 Lasers to Find Land Mines and IEDs....368
8.11.5 Laser Drilling and Analyzing System 369
8.11.6 Terahertz Quantum Cascade Lasers 369
8.11.7 Dogs for IED Detectors....370
8.11.8 Radio Signal....370
8.11.9 Talon II Remote-Controlled Robot/Intelligent Robots....370
8.11.10 Mine Clearing Line Charge....370
8.12 Countering Nuclear and Radiological Threats....371
8.13 Mother Nature and Intelligent-Improvised Explosive Devices to Defeat Low-Tech IEDs, Land Mines, Other Hidden Weapons, and the Enemy....371
8.14 Conclusion 372
References....373

Preface

This book is derived from my doctoral research work and is a revised version of my first book, *Risk Assessment for Water Infrastructure Safety and Security* (2011). The topics covered in this book represent advances in research and development over the past several years. The aim of this book is to present material to convey the *essence* of employing the methodology of the "quantitative psychology of intuitive judgments into risk assessment for homeland and critical infrastructure protection and to improve public perception of risk on terrorism" using pipelines, tunnels, underground rapid rail, and transit systems as examples. The emphasis is on applying *quantitative psychology* in risk management in the area of homeland security and defense. However, as it is a *new*, unproven methodology involving human psychology, it has not yet been utilized in these areas.

The book is divided into eight chapters. Chapter 1 presents the significance of risk and acceptability analyses to protect pipelines, tunnels, underground rails, and transit systems against terrorist attacks. The preparedness as well as the preventive and defensive approaches in this book are intended for man-made disasters, because an *act of God* can only be managed and can never be controlled, unlike terrorist acts. The purpose and objectives are discussed in detail to prepare readers for what is to follow in the subsequent chapters.

Chapter 2 deals with material used for fabricating weapons of mass destruction (WMD) and operations for terrorism including a summary of natural disasters. Natural disasters arising from seismic waves and wind loads are already part of considerations in the structural analysis and design of infrastructures. Engineers should also be aware of the engineering designs and planning and construction of critical infrastructure to ward off terrorist attacks (e.g., impact load of improvised explosive devices on structures), which are covered in this chapter. They should also employ protective and defensive measures to mitigate terrorists from causing large-scale destruction.

Chapter 3 outlines the background and system operations of pipelines, tunnels, underground rails, and transit systems as well as other superspeed futuristic trains (e.g., magnetic levitation, Swissmetro, CargoCap, and tubular rail). It discusses hazards in the event of an explosion as well as the formation and flight of missiles,

dispersion of toxic substances, and dangerous debris released due to demolition of infrastructures. Clandestine tunnels used in times of war, including secret manpower mobilization for WMD production and transshipment and illegal tunnels on borders, are also described in this chapter.

Chapter 4 discusses the risk and vulnerability assessment tools and methodologies used by experts and governmental agencies. It also elaborates on the historical development of cumulative prospect theory.

Chapter 5 deals with the probabilistic risk estimation process, event tree analysis, and fault tree analysis. Terrorism activity scenario developments are illustrated from causative event to prescribing consequence value using examples related to pipelines, tunnels, underground rail and transit systems, clandestine tunnels, and transshipment of WMD materials.

Chapters 6 and 7 form the crux of the book. These chapters describe the meaning and significance of risk acceptability analysis based on quantitative psychology of intuitive predictions for homeland and critical infrastructure protection. It has a vital role to compare alternative solutions and operations or used for policy formulation or to select special features of technologies that are mission critical for the safety and security of assets. Chapter 7 integrates risk assessment methodology with intelligence analysis and military intuitive judgment and provides illustrative examples and graphical presentations of different scenarios. It also introduces the role that the military plays to support civilians in the event of terrorist strikes, including regulations that mandate their missions and limitations.

Chapter 8 reviews preparedness and preventive measures and describes *the need for defensive systems* that can discriminate and terminate terrorists before they can sabotage infrastructures. Technologies and operations to detect illegal tunnels, land mines, and improvised explosive devices currently available and being developed are presented in this chapter. The use of *Mother Nature to support warfare* is briefly discussed in the last part of the chapter.

This work is the culmination of tireless effort and perseverance. I share my thoughts, experiences, and ideas and contribute to improving the safety and security of the homeland. I am honored that Mark Listewnik, senior editor at Taylor & Francis Group, my work organization, and all the people who inspired me have given me a chance to make this a reality.

Acknowledgments

I first express my gratitude to my current mentor, Robert (Bob) Linza, for painstakingly reviewing this book in the midst of his busy schedule and to my editor, Mark Listewnik, senior editor at the Taylor & Francis Group, for giving me the opportunity to write this book and for his never-ending patience regarding the Agency Public Affairs' extensive review. Bob and Mark have been two of my greatest mentors. I thank them for their thoughtful advice and kindness, which helped turn this book into reality.

I acknowledge John Weatherford for his support to this book and my work-related activities; my former mentor, Dr. Timothy Brotherton, for his thoughtful advice and guidance; and Craig Williams for his encouragement. Their work ethic, sense of humor, principles, and leadership qualities have greatly influenced me, and I am very fortunate to be working with them.

I am grateful to Christopher Szkrybalo, Public Affairs and Communications, for the timely approval of this book and to all the prepublication reviewers for their efforts and diligence.

I extend my thanks to Richard O'Hanley, publisher; to Kathryn Everett, project coordinator, for her efforts to keep me on track and for her friendliness; George Kenney, account sales representative; and to all the editorial staff at Taylor & Francis Group for their support and patience.

I am grateful to my former mentor, Dr. Chia Shun Shih—PE, former associate administrator of research, technology, and analysis at the US Department of Transportation and Department of Energy, vice president of PTS International, and retired professor at the University of Texas at San Antonio—for sharing his knowledge about prospect theory in risk acceptability analysis.

I thank my friends Farrah Tacandong and Sareoun Mou Medrano for helping me realize my mission. Special thanks to Stephen W. Goldsmith, DVM, for his focused attitude and sense of humor, which motivated me to finish this book.

I am grateful to Mitch Kruger, computer-aided design expert, and Stephanie Morris for their inspirational advice.

I also extend my thanks to the Society of Hispanic Professional Engineers–Los Angeles Chapter, Robert Guzman and the Hispanic Engineers Business Corporation, as well as the following colleagues at Los Angeles: Rodrigo Garcia, PE, Century Diversified, Inc.; Michael and Mona Trujillo, Golden State Management Services; DeAna Vitela-Hayashi and Dennis Hayashi, AquaBio Environmental Technologies, Inc.; Martin Hershkowitz, Hershkowitz Associates; Noel Plutchak, PG, Priscilla Hibbs; and Dr. Barry Hibbs, for their support to my work.

I express my most sincere thanks to my younger brothers, Romwel and Romcel, for their support; my mom, Marcela; my dad, Romeo Doro-on; and to Anna Liza, Rommel, Fe Nolte, Jean, and Edgar Lao for their unconditional love and support.

Finally, I thank God for having endowed me with multiple talents, such as creative thinking, strength, and endurance, which allowed me to complete this work.

Author

Anna Doro-on, PhD, is a civil service professional and an engineer working in the area of engineering research and technology development. She has many years of extensive experience in the engineering consulting industry and has a knack for engineering computer-aided design software. Her artistic background and expertise at graphic illustration allow her to express difficult engineering perspectives and abstract concepts very clearly. Her work experience includes developing and applying innovative technologies; creating computer-aided designs and civil 3D and graphic illustrations for technical/engineering applications; working with civil/environmental/water resources and in the field of chemical engineering; studying pipelines, underground freight transportation, and tunnel systems; analyzing technical oversights on projects; and conducting research on systems engineering and risk assessment for critical infrastructure with a focus on terrorism, weapons of mass destruction, disaster, and homeland security.

Dr. Doro-on also has experience in assessing the extent of soil and groundwater contamination in complex geologic and hydrogeologic settings; investigating fate and transport of contaminants in soil and groundwater; preparing remedial investigation and feasibility study reports, National Environmental Policy Act (NEPA) permitting; developing remedial action plans; developing cost estimates; and providing project management for hazardous material release sites. She has developed and implemented Resource Conservation and Recovery Act (RCRA) facility investigation work plans and corrective actions. She has also managed several projects related to environmental/water resources engineering, civil engineering, risk assessment, cryogenic technology and chemical engineering, construction management, project management, and loss prevention for power, industrial, and chemical plants. Dr. Doro-on was an adjunct instructor at the University of Texas at San Antonio from 2004 through 2007. She taught courses on civil engineering measurements, surveying, geographic information system, and computer-aided design. She earned a PhD in environmental science and engineering from the University of Texas at San Antonio in 2009, an MS in civil engineering from the University of Texas at San Antonio in 2003, and a BS in civil engineering, specializing in structural and construction engineering, from Ateneo de Davao University in 1999.

Dr. Doro-on published her first book, *Risk Assessment for Water Infrastructure Security and Safety,* in 2011, derived from her PhD dissertation and thoroughly digested the cumulative prospect theory (CPT) related to the definition of risk and perfected the concepts of risk acceptability based on quantitative psychology of intuitive judgments, CPT. Based on a comparison of the incremental acceptable risk determined by the current socioeconomic value versus potential risk of terrorism and disaster, she developed a comprehensive methodology for risk acceptability analysis using "water terrorism" as an illustrative example. As her comprehensive methodology can also be applied to other engineering risk assessments, she has developed many new methods for risk assessment related to homeland security, defense actions, disaster preparedness, and infrastructure security. Dr. Doro-on is a member of the Environmental and Water Resources Institute–American Society of Civil Engineers; INFORMS (Military Application Society, Computing Society and Decision Analysis Society); the Association of Researchers for Construction Management, Europe; Decision Making in Urban and Civil Engineering, Europe; the American Academy of Sciences; the Society of Hispanic Professional Engineers; and the International Society on Underground Freight Transportation.

Chapter 1

Introduction

1.1 Background

Before reading the chapters of this book, the first question that should be asked is "Why is *risk acceptability analysis* (RAA) crucial for critical infrastructure security and defense against terrorism and disaster?" Most experts are aware that risk is defined as a function of the probability of adverse events and dangerous consequences. *Risk of terrorist acts* is measured according to the perceived magnitude of grave consequences and the realized relative weight associated with the probable occurrence of the event by society. Hence, *risk assessment* is routinely employed by security and defense professionals to measure risk levels of threats and disasters. Yet, most of these *standard risk assessments* usually provide evaluation and measurements of the specific risk conditions but do not entirely consider the overall causative risk events, are unable to prescribe consequence values, and most often do not measure acceptable risk based on the quantitative psychology of intuitive judgments. It is true that there is no perfect risk deterrent, while potential threats always exist. Thus, *acceptable risk determination* based on quantitative psychology is important and should be integrated in the decision-making process for security and defense actions.

This book will provide the answers to the question "Why is RAA based on the quantitative psychology of decision-making significant in homeland security and defense?" As engineers, scientists, and defense and security professionals, we have the responsibility to provide technologies and solutions within the designated amount of resources and specific time frame to lessen the impacts of disaster and deter terror attacks or other possible catastrophic events. By performing risk analysis, we may obtain information about the methods to improve protective systems. However, using standard risk evaluation is not enough to determine what risk levels can be allowed; this is where RAA can be utilized. This book will educate readers

about this *new methodology of risk measurements* using rail transit, railroads, oil and gas pipelines, capsule pipelines, and other tunnel systems as illustrative examples for protection against terrorism and disaster.

1.2 Risk Acceptability of Terrorism and Disaster

The bold planning of terrorist attacks on September 11, 2001 (9/11), that devastated the United States and the recent threats of the North Korean and Iranian weapons of mass destruction (WMD) have mobilized government leaders, intelligence communities, and homeland security and defense organizations to significantly upgrade current approaches and to improve the effectiveness of protecting homeland critical infrastructures and allies. Uncertainly, the rapid change has resulted in a disproportionate conversion, in terms of promptness and the total resources put into counterterrorism actions. The outcome is that some areas in national and international security—including rail transit, railroads, oil and gas pipelines, underground freight transportation, and tunnel systems, and porous borders with Canada and Mexico—have been low on the federal government's resources and support priority with the consequence that limited progress has been made to render the United States, its allies, and friendly nations less vulnerable to attack by terrorists. The enemies, as a devious, clever, and adaptive system, would be perceived to have used this opportunity to plan targets and calculate attacks. Systematic protection strategies are needed so that decision makers and experts can incorporate risk acceptability in providing quantitative tools for terrorism threat assessment and warnings.

1.3 Objective

The objective of this book is to present and develop a risk assessment methodology based on *cumulative prospect theory*—a quantitative psychology assessment process for the analysis of threats of terrorism against rail transit, railroads, railways, oil and gas pipelines, and underground freight transportation through pipelines and other tunnel systems. The engineering, environmental, and economic impacts will be analyzed in detail for terrorist attacks and disaster, including both direct and collateral damage.

1.4 Scope

The scope of this book includes the following topics: development of an integrated approach of risk assessment based upon *cumulative prospect theory*; review of legal and regulatory requirements related to the security policy of rail transit, railroads, railways, oil and gas pipelines, underground freight transportation through pipelines, and tunnel systems against terrorism and disaster; illegal transport of WMD

identification; models of secret/illegal underground tunnels and subterranean infrastructures by adversaries; application of an integrated model to the risk assessment of pipelines, rail, tunnels, and unlawful distribution of WMD as an illustrative example for the approach. Specifically, the following will be presented:

- Evaluation of terrorism hazards on oil and gas pipelines, rail transit, railroads, railways, underground freight transportation through pipelines and tunnel systems
- Development of *risk estimation model* based on the event tree analysis
- Development of terrorism activity scenario
- Development of *fault tree analysis* for potential terrorism activities
- Development of an integrated approach for the risk analysis embedded with cumulative prospect theory for acts of terrorism against oil and gas pipelines, rail transit, railroads, railways, underground freight transportation through pipelines, and other tunnel systems of urban areas
- Hazard evaluations of oil and gas pipelines explosion, and blasting of rail transit and other mode of underground freight transportation near population and urban areas
- Review of the Department of Defense (DoD) policy requirements for military support to civilian law enforcement and homeland in the event of terrorist attacks
- Review and application of standard qualitative/quantitative processes, operational formulations, and models recommended by other renowned authors, private industry consultants, Department of Homeland Security, DoD, and some of the governmental agencies
- Evaluation of current intelligence and military operations for security and detection of illegal transport of WMD by enemies
- Development of a concise *strategic intelligence analysis* integrated with cumulative prospect theory
- Evaluation of terrorism threats and warnings
- Development of preventive measures, emergency preparedness plans, economic analysis, and protocols

1.5 Purpose

Terrorist attacks against oil and gas pipelines, rail transit, underground capsule pipelines, and tunnel systems adjacent or near urban area or other major infrastructures could impact the public in the following ways:

- Cause mass casualties and catastrophic health effects due to the release of hazardous materials and burst of missiles of sharp objects and debris
- Create chaos in regional, national, and/or international security

- Cause damage to public morale and confidence
- Contaminate the environment and damage natural resources
- Disrupt the industry and commercial infrastructure that depend on oil and gas energy sources, rail transit, tunnels, and other modes of freight transportation systems
- Cause regional or national economic and financial chaos to infrastructure owners and homeland from the destruction of oil and gas distribution pipelines, rail transit, and tunnel systems which connect large urban regions
- Create a need to remediate the environment from the release of massive hazardous or radioactive materials
- Create a need to replace rail transit and tunnel systems that connect large metropolitan areas and states
- Result in significant costs for replacement of pipelines, underground high-speed transportation, and tunnel systems, which likely could weaken the US economy

Because any of these impacts could have serious consequences, the United Sates, its allies, and friendly nations should be concerned about terrorist attacks using improvised explosive devices and large-scale WMD. Accordingly, this study is required to recognize the prospective events of terrorism including secret tunnels and illegal transport of WMD materials. The uncovering of these events may lead to strategic improvements in critical infrastructure protection not only in the United States but also in other countries, making it more difficult for the attacks to succeed and maximizing the acceptability of terrorist attacks. The safeguards employed include change in policy, incorporation of intrusion detection technology, increased surveillance, heavily required military support, and improved intelligence. In addition to strategic security enhancements, tactical defense improvements to critical infrastructure can be rapidly implemented to neutralize potential attacks and disasters.

Chapter 2

Hazards, Terrorism, and Weapons of Mass Destruction on Pipelines, Tunnels, and Underground Rail and Transit Systems

2.1 Introduction

This chapter introduces terrorism, weapons of mass destruction (WMD), and natural disasters on oil and gas pipelines, tunnels, underground rail, and transit systems. Additionally, the terrorism network operations will be discussed briefly in this chapter. Common *explosives* and blasting components of improvised explosive devices (IEDs) will be presented. It is critical to improve weapons technical intelligence (WTI) capabilities and strategies to effectively investigate, detect, and deter IEDs. IEDs are responsible for numerous American combat casualties including civilians in Iraq and Afghanistan (Doro-on 2011). The Department of Homeland Security (DHS) has no specific and detailed information to indicate that IEDs or any other types of improvised weapon systems are currently being planned for use

in the United States (Doro-on 2011). Thus, this chapter provides the basic WMDs and their design, specifications, and characteristics so that we can identify what improvements we need to offer for protection against terrorism and disaster.

2.1.1 Terrorism and Disasters against Pipelines, Tunnels, Underground Rail, and Transit Systems

Oil and gas pipelines, tunnels, underground rail, and transit systems are critical to the continued functioning of every nation, society, and economy, serving as an efficient way of delivering hazardous materials (HAZMAT), energy sources, water supply, agricultural and industrial products, and disruption for any period could cause public panic. IEDs, rocket-propelled grenades, or other types of improvised weapons can be potentially used for attacking these infrastructures. Chapter 3 provides more information related to man-originated disasters on these infrastructures.

2.2 Understanding the Basic Structure of Terror Organization

The following sections provide a very basic description of the terrorism development and operation for engineers.

2.2.1 Basic Recruitment Operations

The most common way that terror members are recruited is through the use of religious or known to be godly doctrines embedded with twisted political concepts. One has to be aware that recruitment does not only happen within the society known to support and harbor terror organizations; it can also exist in professional or academic organizations situated in an academic environment.

2.2.2 Terror Aspirant and Self-Radicalization

A terror aspirant is an individual who is willing to self-radicalize and participate in an organization strongly against a political norm, regime, government, or state. Some of these terror aspirants do not originally intend to be part of terror organizations; they want to join the organization out of curiosity, gain self-recognition, and acquire brotherhood support that they do not find elsewhere. Once they are in the designated terror system, the members who are aware of the real operations will persuade these newly recruited members to be deeply involved in the actual purpose of the organization and send them to certain site camps to indoctrinate them.

2.2.3 Terror Member

A terror member is a fully indoctrinated and radicalized individual who has sincerely devoted his life for the mission of the organization. In a larger perspective, a terror leader of an entire state can persuade his people to turn against another state or government, making them dedicate their lives to support the terror leader's goals without hesitation or questioning the real mission. The mechanism of indoctrination is through psychological and physical training within a hostile environment.

2.2.4 Terror-Suicide Bomber

There are several factors that are taken into consideration for recruiting a terror-suicide bomber as follows: (a) attacking the vulnerability of an individual (e.g., an individual who has lost hope of love or respect from their love ones and is desperate to acquire financial reward); (b) completely indoctrinating an individual with godly principles and religious doctrines integrated with inappropriate family values and incorrect political ideas; (c) motivating an individual to kill and/or create damage knowing that he or she might have to die in the process, for the mission that he or she believes is purely part of God's willing and purpose for the benefit of their own society.

2.2.5 Technical Bomb and Improvised Explosive Devices Developer

There are terrorist members who are trained to develop technical bombs and IEDs. The supplies are typically smuggled from neighboring countries. Corruption and deficiency in regulations are major problems in some nations, where law enforcement or armed forces members and even politicians sell firearms and materials for weapons illegally. Most of these explosive devices are built by corrupt soldiers or officers supporting terrorist organizations in exchange of financial reward or security.

2.2.6 Terrorists Specializing in Chemical Threat

Terrorist members who are capable of acquiring, developing, and handling chemical weapons usually undergo clandestine training within the terror organization. Not all terrorist members are able to perform chemical terrorism due to the complexity of delivery. The lead terrorist who is in charge of this capability would have usually acquired practical training and/or education related to chemistry or chemical engineering. Large terrorist groups also seek expertise from active or retired chemical scientists or engineers willing to participate in providing secret consultancy.

2.2.7 Terrorists Specializing in Biological Threat

It is difficult to develop and produce biological threats in large quantity for weapon of mass genocide. A devious nation would likely coordinate with other terrorist groups or other rebellious nations to obtain, manufacture, and generate this capability. Large terrorist groups and rebellious nations seek expertise or hired scientists or engineers who are capable of mass producing biological threats.

2.2.8 Terrorists Specializing in Radiological and Nuclear Weapons

Radiological and nuclear weapons are the most sophisticated, expensive, and dangerous possessions that terrorist organizations and rebellious nations can have. Acquiring and handling radiological and nuclear weapons require special skills. Terrorist members or supporters who are considered experts in nuclear weapon systems should have had academic and professional training in the subject. Due to corruption and weak enforcement of regulatory standards in terms of prohibiting nuclear bomb materials being manufactured and distributed illegally in other foreign nations, it would be difficult to mitigate rebellious nations and large terrorist organizations in accessing nuclear materials.

2.2.9 Terrorist Intelligence Information and Reconnaissance Operation

Terrorist organizations and rebellious nations have agents and currently have technological means to explore essential target areas to collect information that can aid them in their weapons productions, and improve their armed forces and combat strategies for future conflicts and attacks.

2.2.10 Terror Planner and Military Operation Planner

Large terrorist organizations have designated terror planners. They are responsible for preparing the potential time frame, place, synchronization, and weapons to be used for attacks similar to the 9/11 terrorist attacks. Terrorist organizations constantly seek to gain tactical military operations from their supporters and allies. Oftentimes, they gain information to model their military strategies from military officers and public officials who may likely have a similar ideology.

2.3 Weapons of Mass Destruction

According to the US House of Representatives—Committee on Homeland Security (HRCHS), in 2013, chemical, biological, radiological, and nuclear (CBRN) weapons, known as *WMD*, pose a daunting challenge to homeland security because of their

potentially catastrophic consequences. The Department of Defense (DoD), in 1998, stated that WMD include any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release of toxic or poisonous chemicals or their precursors, a disease organism, or radiation or radioactivity. It is widely believed that terrorists are actively seeking to acquire, build, and use a WMD against the US homeland (US HRCHS 2013). After all, the United States faced the potential mass destruction from nuclear weapons by the former Soviet Union for nearly half a century during the Cold War (US DoD 2007). Moreover, the disintegration of the former Soviet Union increased concerns about the protection, control, and accountability of WMD, related materials, and technologies, and the potential unemployment and proliferation of thousands of scientists skilled in this filled (US DoD 1998). Transnational threats arising from the collapse of the Eastern Bloc, including the development of chemical–biological capabilities by terrorist organizations, have increased the potential for attacks within our borders (US DoD 1998). The growing spread of WMD provides small groups of individuals with the ability to deliver devastating harm to the United States (US DoD 2007).

The United Nations (UN), in 2012, stated that the North Atlantic Treaty Organization (NATO) places a high priority on preventing the proliferation of WMD and defending against CBRN threats and hazards and the Alliance will work actively to prevent proliferation of WMD by state and non-state actors. At the 2010 Lisbon Summit, NATO Heads of State and Government called for universal adherence to, and compliance with, the Nuclear Nonproliferation Treaty (NPT) and the additional protocol to the International Atomic Energy Agency Safeguard Agreement, and called for full implementation of the United Nations Security Council Resolution (UNSCR) 1540 (UN 2012). Within the NATO Response Force (NRF), the multinational Combined Joint CBRN Defence Task Force, including the CBRN Joint Assessment Team, is the key asset to protect from, and respond to, an attack or event involving CBRN materials (UN 2012). NATO will work actively to prevent the proliferation of WMD by state and non-state actors through an active political agenda of arms control, disarmament, and nonproliferation as well as by developing and harmonizing defense capabilities and, when necessary, by employing these capabilities consistent with political decisions in support of nonproliferation objectives (NATO 2013). In the field of WMD disarmament, NATO has, with the changes in the security environment since the end of the Cold War, dramatically reduced the number of nuclear weapons stationed in Europe and our reliance on nuclear weapons in the NATO strategy. No NATO member country has a chemical or biological weapons program (NATO 2013). Additionally, the Allies are committed to destroy any stockpiles of chemical agents and have supported a number of partner countries in such activity (NATO 2013). The NATO–Russia cooperation is of strategic importance as it contributes to creating a common space of peace, stability, and security (NATO 2013).

Countering the WMD threat requires a risk-based, layered approach, in which we would aim to understand and anticipate the threat, control access to and movement

of weapons, and expand and strengthen our capabilities to detect, protect against, mitigate, respond to, and recover from an attack (US HRCHS 2013). Improving intelligence is a necessary enabler for all other steps to reduce WMD vulnerability (US DoD 2007). Still, DoD can help create a truly integrated WMD intelligence community focused on improving strategic knowledge through innovative collection, dramatically revitalized analysis, and a war room mentality for attacking the problem and influencing the plans and perspectives of relevant actors (US DoD 2007). Since 1993, DoD has been laying greater emphasis on the nuclear, biological, and chemical (NBC) threat in its planning and policy documents (US GAO 2000). For instance, the defense planning guidance provided by the Secretary of Defense to DoD components has placed increasing emphasis on the NBC threat, particularly the biological and chemical threat, and the importance of preparing for it. The 1998 and 1999 planning guidance state that countering the NBC threat will be given high priority in defense planning (US GAO 2000). To better manage its counterproliferation efforts, DoD has taken steps to improve its organizational structure. For example, the Air Force has established a central headquarters office for counterproliferation, which is the focal point for all Air Force counterproliferation activities, including doctrine, strategy, policy, and requirements (US GAO 2000). This office has developed a master plan to provide the overarching guidance to enable the Air Force to meet its counterproliferation goals and a long-term plan to guide the development and acquisition of improved counterproliferation capabilities (US GAO 2000). The NPT entrusts the International Atomic Energy Agency (IAEA) with specific roles as the international safeguards inspectorate and as a multilateral channel for transferring peaceful applications of nuclear technology (IAEA 2003). It is instructive that the majority of suspected efforts to acquire WMD are to be found in the Middle East, a hotbed of instability for over half a century (IAEA 2003). Regarding the Democratic People's Republic of Korea (DPRK), IAEA safeguard inspectors are no longer in the country, and the IAEA Board has reported the DPRK's continuing noncompliance with its safeguards agreement to the UN Security Council and General Assembly (IAEA 2003). The following sections present most of the explosives, and chemical and biological agents used as WMD and natural disasters.

2.4 Chemical Explosives

Explosives are made up of chemical compounds with oxygen in the materials to produce detonation when chemical reaction occurs. The Lawrence Berkeley National Laboratory (LBNL), in 2010, stated that high explosives are divided into two classes: primary and secondary. Primary explosives are extremely sensitive to impact, friction, heat, or electrostatic sources and they are generally used in detonators or to trigger larger charges of less sensitive secondary explosives (LBNL 2010). Secondary explosives are relatively insensitive to shock friction and heat, and may burn when exposed

to heat or flame in small, unconfined quantities but normally require initiation from a primary explosive to detonate (LBNL 2010). Low explosives deflagrate quickly.

Explosive materials include explosives, blasting agents, and detonators. A list of explosive materials determined to be within the coverage of 18 USC Chapter 40, Importation, Manufacture, Distribution, and Storage of Explosive Materials is issued at least annually by the Director of the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) of the Department of Justice. The US Department of Transportation (DOT) classifications of explosive materials used in commercial blasting operations are not identical with the statutory definitions of the Organized Crime Control Act of 1970, Title 18 USC Section 841. Title 49, Transportation Code of Federal Regulations (CFR), Chapter 1, classifies chemical explosives into three categories: class A explosives (detonating, or otherwise maximum hazard), class S explosives (flammable hazard), class C explosives (minimum hazard); and oxidizing material (a substance that yields oxygen readily to stimulate the combustion of organic matter). Detailed categories of chemical explosives commonly used by terrorist enemies are presented in the following sections.

2.4.1 Acetone Peroxide

Acetone peroxide (tricycloacetone peroxide or triacetone triperoxide; Chemical Abstract Service [CAS] number 17088-37-8; known as the *mother of Satan* by terrorist enemies) is the most favorable explosive material used by terrorists; however, it should not be easily accessed by any individual without background investigation. Acetone peroxide is a white crystalline solid formed from acetone in sulfuric acid solution when acted upon by 45% hydrogen peroxide. Its properties are comparable to those of primary explosives. Acetone peroxide is not normally used in practice because of its tendency to undergo sublimation, although it can be found in hazardous waste sites. It is highly susceptible to heat, friction, and shock. However, it is a strong weapon for destroying portions of oil and gas pipelines and underground high-speed rail systems, so engineers need to produce preventive measures that can protect from enemy usage of this material in infrastructures. It was used as the chemical explosive in the July 2005 London bombings during the morning rush hour. The chemical compositions are commercially accessible. The cyclic dimer ($C_6H_{12}O_4$), an open monomer, and a dimer are also formed, but under special conditions, the cyclic trimer ($C_9H_{18}O_6$) is the primary product. The criteria and characteristics of acetone peroxide include but are not limited to the following: oxygen balance, −151.3%; explosive velocity, 3.29 mile/s; lead block test, 250 cm^3/10 g; melting point, 91°C; impact sensitivity, 0.3 N·m; and friction sensitivity, 0.1 N. Enemies and self-radicalized individuals generally initiate terrorism during rush hours. Again, preventive and defensive approaches should be designed and prepared according to the calculated time frame and distance of the explosion. There are no current immediate defensive systems employed for chemical explosive attacks.

2.4.2 Ammonium Nitrate

Ammonium nitrate (NH_4NO_3; AN; CAS number 6484-52-2) is hygroscopic and water-soluble. The US DHS, in 2013, developed the Ammonium Nitrate Security Program in response to direction from the Congress to regulate the sale and transfer of ammonium nitrate by an ammonium nitrate facility to prevent misappropriation or use of AN in an act of terrorism. Each purchaser and seller will be required to apply for an Ammonium Nitrate (AN) Registered User Number with the Department, and each applicant will be screened against the Terrorist Screening Database (TSDB) (US DHS 2013). Additionally, the Bureau of ATF, 2013, is primarily concerned with law enforcement and regulatory duties, while also striving to work and consult with the industries it regulates and the businesses, agencies, and groups that affect it.

Hence, even though there is a regulatory requirement enforcing that no individual may acquire AN conveniently, terrorists and criminals are able to acquire AN as a weapon of destruction through the agricultural industry. AN is commonly used to make improvised explosive weapons in Afghanistan and it was used in the notorious 1995 federal building bombing in Oklahoma City. After the 1995 bombing of the Murrah Federal Building in Oklahoma City, Oklahoma, ATF formed an alliance with The Fertilizer Institute (TFI) and other agriculture industry members to put forward the *Be Aware for America* program (ATF 2013). This voluntary program encourages agriculture industry members to report any suspicious activities or thefts of ammonium nitrate—a precursor chemical often sought by those with criminal intent—to ATF (ATF 2013).

AN fertilizer is standardly used in the agriculture sector, and has a chemical composition of 27% nitrogen and 8% calcium carbonate, which is usually susceptible to cake, and the resulting difficulties are avoided by transforming the material into *prills* (prills are small aggregate materials formed from a melted liquid). It is commercially produced as dense prills and as porous prills employed for industrial explosives such as tunneling and/or mining after milling.

AN explosives are composed of AN with carbon carriers (e.g., coal or wood meal) and sensitizers such as *nitroglycol* or trinitrotoluene (TNT) with aluminum powder in it to produce a stronger explosion. Higher density (e.g., 0.9–1.0 g/cm^3) and better water resistance are obtained using gelatinous AN explosives and adding hydrophobic agents. They are based on AN and 20%–40% gelatinized nitroglycol or a nitroglycerine–nitroglycol mixture with an approximate density of 1.6 g/cm^3. Many allowed and regulated explosives are AN in powder form or gelatinous explosives with added rock salt or potassium chloride, which lowers their explosion temperature. Because it tends to be very difficult to detonate, another high explosive or strong industrial or military blasting cap—a #8 cap and 12 oz of *pentaerythritol tetranitrate* (PETN) or hexahydro-1,3,5-trinitro-1,3,5-triazine (RDX)—is needed to detonate it; it melts at 180°C, holds 378 cal/g of energy, and has a detonating velocity of 3460 m/s. Table 2.1 provides the detailed characteristics and specifications of AN.

Table 2.1 Characteristics and Specifications of Ammonium Nitrate

Color: Colorless crystals, white/light gray solid
Molecular weight: 80
CAS number: 6484-52-2
Energy of formation: –4428.0 kJ/kg
Enthalpy of formation: –4567.0 kJ/kg
Oxygen balance: +19.99%
Nitrogen content: 34.98%
Volume of explosion gases: 980 L/kg
Heat of explosion: (H_2O liq.) 479 kJ/kg (H_2O gas) 1441 kJ/kg
Melting point: 169.6°C = 337.3°F
Lead block test: 180 cm^3/10 g
Deflagration point: Starts decomposition at the melting point of 169.6°C; completes approximately at 210°C (boiling point)
Temperature of decomposition: completes at 210°C
Impact sensitivity: up to 50 N·m
Friction sensitivity: 353 N pistil load no reaction
Critical diameter of steel sleeve test: 1 mm

Note: See USEPA (2010d), Meyer et al. (2002), Akhavan (2004), ATF (1984, 2010).

2.4.3 Ammonium Nitrate–Fuel Oil

Ammonium nitrate–fuel oil (NH_4NO_3, ANFO; 1,3,5-trinitro-1,3,5-triazacyclohexane; CAS No. 6484-52-2) is a tertiary explosive or blasting agent soluble in water and composed of AN and liquid hydrocarbons which is commercially produced as porous prills. These are granules solidified from the liquid melt, sufficiently porous to absorb up to 6% of the oil, which is the quantity required to maintain oxygen balance. Because of its ready availability and cheap material cost, ANFO has been used extensively as the main charge in improvised weapons around the world and is the most common commercial explosive (NCTC 2013). The optimum blend for ANFO (if properly prepared) could yield greater explosive power than TNT (NCTC 2013).

2.4.4 Cyclonite (RDX)

Cyclonite ($C_3H_6N_6O_6$; Royal Demolition Explosive, RDX) is a white, crystalline solid used in mixture with other explosives/blasting agents and plasticizers,

phlegmatizers, or desensitizers. RDX can be dissolved in acetone, ether, and ethanol, but is insoluble in water. *Cyclohexanone*, *nitrobenzene*, and *glycol* are solvents at elevated temperatures. Its *detonation velocity* at a density of 1.76 g/cm^3 is quantified as 8750 m/s. The chemical reaction of concentrated nitric acid with hexamine produces RDX. The decomposition temperature is 170°C and the melting point is 204°C. Based on testimony in the US Court of Appeals for the ninth circuit, dated February 2, 2010, Ahmed Ressam, the Al-Qaeda millennium bomber, used a small quantity of RDX as one of the components in the explosives that he used to bomb Los Angeles International Airport on New Year's Eve 1999; the combined explosives could have produced a blast greater than that produced by a devastating car bomb. RDX was the main component used in the 2006 Mumbai, India, train bombings. Table 2.2 presents the characteristics and specifications of RDX.

2.4.5 Dingu and Sorguyl

Dingu and *sorguyl* were introduced by the *Société Nationale des Poudres et Explosives*, Sogues, France (Meyer et al. 2002). The reaction between glyoxal and urea produces *glycolurile*. Once glycolurile undergoes the dinitration process, it produces dingu. The characteristics of dingu are presented in Table 2.3. It is easily decomposed by alkaline hydrolysis. It is stable in contact with neutral or acid water. It is insoluble in molten TNT but soluble in *dimethylsulfoxide*. Nitration with nitric acid and nitrogen pentoxide can generate sorguyl. Nitro derivatives of glycolurile have recently attracted renewed interest because sorguyl has proven to be one of the most powerful modern explosives (Boileau et al. 1975). Sorguyl has high density and high detonation velocity, which can be used by terrorists for attacking tubular rails and above ground rapid transits. Dingu and sorguyl are not very common in the United States and not easily detected onsite. Sorguyl is not hygroscopic, decomposes easily by hydrolysis (decomposes when mixed with molten TNT), and is insoluble in both hydrocarbons and chlorinated hydrocarbons. The characteristics and specifications of dingu and sorguyl are presented in Tables 2.3 and 2.4.

2.4.6 Hexamethylenetetramine Dinitrate

Hexamethylenetetramine dinitrate is soluble in water but insoluble in alcohol, ether, chloroform, and acetone. It is usually made from hexamethylenetetramine and nitric acid; it is an important precursor of primary explosives. Table 2.5 provides the characteristics and specifications of hexamethylenetetramine dinitrate.

2.4.7 Hexanitroazobenzene

2,2′,4,4′,6,6′-Hexanitroazobenzene (CAS number 19159-68-3) is normally created from *dinitrochlorobenzene* and *hydrazine*. Oxidation and nitration of

Table 2.2 Characteristics and Specifications of RDX

Color: Colorless crystals
CAS number: 121-82-4
Empirical formula: $C_3H_6N_6O_6$
Molecular weight: 222.1
Energy of formation: +401.8 kJ/kg
Enthalpy of formation: +301.4 kJ/kg
Optimum oxygen balance: –21.6%
Optimum nitrogen content: 37.84%
Volume of explosion gases: 903 L/kg
Heat of explosion (H_2O liq.): 5647 kJ/kg (H_2O gas): 5297 kJ/kg
Heat of detonation (H_2O liq.): 6322 kJ/kg
Specific energy: 1375 kJ/kg
Density: 1.82 g/cm^3
Melting point: 204°C
Heat of fusion: 161 kJ/kg
Lead block test: 480 cm^3/10 g
Detonation velocity, confined: 8750 m/s
Impact sensitivity: 7.5 N·m
Friction sensitivity: 120 N

Note: See USEPA (2010e,f), Meyer et al. (2002), ATF (2010), Akhavan (2004).

tetranitrohydrazobenzene can also produce *hexanitroazobenzene* (Table 2.6). It is a strong underwater explosive.

2.4.8 Hexanitrodiphenylamine

Hexanitrodiphenylamine is mostly toxic and a poisonous underwater explosive with TNT and aluminum powder. It is less powerful than *hexanitroazobenzene*. Additionally, it is insoluble in water and most organic solvents, and forms sensitive acid salts. It is prepared by nitration of *asym-dinitrodiphenylamine* and is formed by condensation of dinitrochlorobenzene with aniline. It is an explosive with a relatively low sensitivity to heat and has been used as a precipitant for

Table 2.3 Characteristics and Specifications of Dingu

Color: Colorless
Empirical formula: $C_4H_4N_6O_6$
Molecular weight: 232.1
Oxygen balance: –27.6%
Nitrogen content: 36.2%
Density: 1.94 g/cm^3
Detonation velocity, confined: 7580 m/s
Impact sensitivity: 5–6 N·m
Decomposition begins at 266°F
Friction sensitivity: up to 300 N

Note: See Agrawal and Hodgson (2007), Meyer et al. (2002), Boileau et al. (1975), Emeury and Girardon (1980).

Table 2.4 Characteristics and Specifications of Sorguyl

Color: Colorless
Empirical formula: $C_4H_2N_8O_{10}$
Molecular weight: 322.1
Oxygen balance: +5%
Nitrogen content: 34.79%
Density: 2.01 g/cm^3
Detonation velocity, confined: 9150 m/s
Impact sensitivity: 1.5–2 N·m
Deflagration point: 459°F

Note: See Agrawal and Hodgson (2007), Meyer et al. (2002), Boileau et al. (1975).

potassium. The characteristics and specifications of hexanitrodiphenylamine are presented in Table 2.7.

2.4.9 Hexanitrohexaazalsowurtzitane

The *hexanitrohexaazalsowurtzitane* or CL-20 (CAS number 135285-90-4) is obtained by condensing glyoxal with benzylamine to produce *hexabenzylhexaazaisowurtzitane*. It is one of the most energetic organic explosives due to its high

Table 2.5 Characteristics and Specifications of Hexamethylenetetramine Dinitrate

Color: Colorless crystals
CAS number: 100-97-0
Empirical formula: $C_6H_{14}N_6O_6$
Molecular weight: 266.2
Energy of formation: –1296.6 kJ/kg
Enthalpy of formation: –1417.7 kJ/kg
Oxygen balance: +78.3%
Nitrogen content: 31.57%
Volume of explosion gases: 1081 L/kg
Heat of explosion: (H_2O liq.) 2642 kJ/kg (H_2O gas) 2434 kJ/kg
Melting point: 169.6°C = 316°F
Lead block test: 220 cm^3/10 g
Decomposition begins at melting point; completes at 316°F
Impact sensitivity: up to 50 N·m no reaction
Friction sensitivity: 240 N pistil load reaction

Note: See Meyer et al. (2002), ATF (2010).

Table 2.6 Characteristics and Specifications of Hexanitroazobenzene

Color: Orange red
CAS number: 19159-68-3
Empirical formula: $C_{12}H_4N_8O_{12}$
Molecular weight: 452.2
Oxygen balance: –49.7%
Nitrogen content: 24.78%
Melting point: 430°F

Note: See US Naval Technical Mission to Japan (1945), Meyer et al. (2002), ATF (2010).

Table 2.7 Characteristics of Hexanitrodiphenylamine

Color: Yellow crystals
CAS number: 131-73-7
Empirical formula: $C_{12}H_5N_7O_{12}$
Molecular weight: 439.2
Energy of formation: +162 kJ/kg
Density: 1.64 g/cm^3
Enthalpy of formation: +94.3 kJ/kg
Specific energy 1098 kJ/kg
Optimum oxygen balance: +52.8%
Detonation velocity: 7200 m/s at a density of 1.6 g/cm^3
Optimum nitrogen content: 22.33%
Volume of explosion gases: 791 L/kg
Heat of explosion: (H_2O liq.) 4075 kJ/kg (H_2O gas) 4004 kJ/kg
Melting point: 464°F–466°F
Lead block test: 325cm^3/10 g
Temperature of decomposition: 316°F–471°F
Impact sensitivity: 7.5 N·m pistil load no reaction
Friction sensitivity: 353 N pistil load reaction
Acetone mixture: not more than 0.1%
Insoluble in 1:3 pyridine (C_5H_5N, an important solvent and reagent)

Note: See USAAF (1994), Meyer et al. (2002), ATF (2010), US Naval Technical Mission to Japan (1945).

density and detonation velocity, which is close to or can exceed 10,000 m/s. It can be used as one of the IED components to destroy a portion of a large metropolitan area. The characteristics and specifications of CL-20 are presented in Table 2.8.

2.4.10 Lead Azide

Lead azide ($Pb(N_3)_2$; CAS number 13424-46-9) is poisonous, insoluble in water, and resistant to heat and moisture. It is prepared by reacting sodium azide and

Table 2.8 Characteristics and Specifications of CL-20

Color: White crystalline solid
Empirical formula: $C_6H_6N_{12}O_{12}$
Molecular weight: 438.19
Energy of formation: +1005.3 kJ/kg
Density: 2.04 g/cm^3
Enthalpy of formation: +920.5 kJ/kg
Specific energy: 1323 kJ/kg
Optimum oxygen balance: –10.95%
Optimum nitrogen content: 38.3%
Heat of explosion: (H_2O liq.) 6314 kJ/kg (H_2O gas) 6084 kJ/kg
Melting point: 195°C
Impact sensitivity: 4 N·m
Friction sensitivity: 48 N

Note: See Simpson et al. (1997), Meyer et al. (2002), Lee et al. (2001), Lee and Jaw (2006).

lead nitrate; production of large crystals may occur and should be mitigated for safety from potential explosion during the preparation by precipitation with dextrin or polyvinyl alcohol. Flammability can be improved by adding flammable additives, such as *lead trinitroresorcinate* (lead trinitroresorcinate is a slurry or wet mass of orange-yellow crystals, which is a weak but highly sensitive explosive). Hence, water does not reduce this explosive's impact sensitivity. The characteristics and specifications of lead azide are presented in Table 2.9.

2.4.11 Lead Styphnate

Lead styphnate (or lead trinitroresorcinate; CAS number 15245-44-0) is sensitive to fire, can readily ignite by static discharges from the human body, is insoluble in water, and is moderately soluble in acetone and ethanol. Consequently, it is usually employed as an initiating explosive, with lead azide forming the detonator charge; this is unlikely to be utilized by terrorists in attacking large urban areas due to its very high ignition sensitivity and requires safety handling and transporting procedures where authorities are vigilant to suspicious activities. Table 2.10 shows the characteristics and specifications of lead styphnate.

Table 2.9 Characteristics and Specifications of Lead Azide

Color: Colorless crystals
Molecular weight: 291.3
Energy of formation: +1663.3 kJ/kg
Density: 4.8 g/cm^3
Enthalpy of formation: +1637.7 kJ/kg
Net content as $PbCrO_4$: not less than 91.5%
Optimum oxygen balance: +5.5%
Detonation velocity: depends on the density (e.g., 4500 m/s at a density of 3.8 g/cm^3)
Optimum nitrogen content: 28.85%
Volume of explosion gases: 231 L/kg
Explosion heat: 1638 kJ/kg
Melting point: 464°F–466°F
Lead block test: 325 cm^3/10 g
Temperature of decomposition: completes at 316°F
Impact sensitivity: 2.5–4 N·m (pure); 3.0–6.5 N·m (dextrinated)
Friction sensitivity: 0.1–1 N
Moisture content: 0.3%
Water solubility 1%
Lead content: 68%
Deflagration point: 350°C
Bulk density: 1.1 g/cm^3

Note: See Verneker and Forsyth (1968), Meyer et al. (2002), ATF (2010), McNicol (1966).

2.4.12 Mercury(II) Fulminate

Mercury(II) fulminate (CAS number 628-86-4) is toxic and highly sensitive to friction and shock. It is water-insoluble and can be phlegmatized by the addition of fats, oils, or paraffin. It is prepared by dissolving mercury in nitric acid with 95% ethanol. Then, energetic gas and crystals are produced; crystals are filtered by suction

Table 2.10 Characteristics of Lead Styphnate

Color: Orange–yellow to dark brown crystals
CAS number: 15245-44-0
Empirical formula: $C_6H_3N_3O_9Pb$
Molecular weight: 468.3
Energy of formation: –1747.2 kJ/kg
Density: 3.0 g/cm^3
Enthalpy of formation: –1786.9 kJ/kg
Optimum oxygen balance: –18.8%
Detonation velocity: 5200 m/s at a density of 2.9 g/cm^3
Optimum nitrogen content: 8.97%
Volume of explosion gases: 231 L/kg
Lead block test: 130 cm^3/10 g
Impact sensitivity: 2.5–5.0 N·m
Moisture content: 0.15%
Net content: 98%
Water solubility not more than 1%
Lead content: 43.2%–44.3%
Ca, Mg: 0.5%
Na: 0.07%
pH: 5–7
Deflagration point: 518°F
Bulk density: 1.3–1.5 g/cm^3

Note: See Jiang (2005), Meyer et al. (2002), ATF (2010), Ledgard (2002).

and washed until neutral after the reaction. The mercury(II) fulminate product is obtained as a small brown to gray pyramid-shaped crystal, the color of which is caused by the presence of colloidal mercury. It is normally stored underwater and dried at 104°F shortly before use. Its characteristics and specifications are presented in Table 2.11.

Table 2.11 Characteristics and Specifications of Mercury(II) Fulminate

Color: Colorless
CAS number: 628-86-4
Empirical formula: $Hg(CNO)_2$
Molecular weight: 284.6
Energy of formation: +958 kJ/kg
Density: 4.42 g/cm^3
Enthalpy of formation: +941 kJ/kg
Optimum oxygen balance: –11.2%
Nitrogen content: 9.84%
Impact sensitivity: 1.0–2.0 N·m
Net content not less than 98%
Water solubility not more than 1%
Deflagration point: 330°F

Note: See Beck et al. (2007), Meyer et al. (2002), Perry and Phillips (1995).

2.4.13 Nitrocellulose

Nitrocellulose (CAS number 9004-70-0) is prepared by the reaction of a nitrating mixture on high-quality cellulose prepared from wood pulp. The crude nitration product is first centrifuged to remove the bulk of the acid, after which it is stabilized by preliminary and final boiling operations (Meyer et al. 2002). The nitration processes are resumed while measured amounts of nitric acid and anhydrous sulfuric acid are applied to regulate the spent acid. Standard nitrocellulose types are manufactured and blended with the desired nitrogen content. Blasting soluble nitrocotton (dynamite nitrocotton; 12.3% nitrogen) is held at high viscosity to maintain good gelatinizing properties. All nitrocelluloses are soluble in acetone. In addition, it is a highly flammable compound formed by nitration of cellulose. Most airport x-ray machines may not be able to detect nitrocellulose, although another type of technology called a *trace detection* machine can. Most underdeveloped countries may not have technologies to detect nitrocellulose; terrorists will be able to pass through their security system and can hijack aircrafts heading to the United States to carry out a series of attacks. Table 2.12 shows the characteristics and specifications of nitrocellulose.

Table 2.12 Characteristics and Specifications of Nitrocellulose

Color: White fibers
CAS number: 9004-70-0
Empirical formula: $C_{12}H_{14}N_6O_{22}$
Nitration grade: 14.14%
Optimum nitrogen content: 13.4% or 13.5% with anhydrous phosphoric acid
Molecular weight of the structure unit: 324.2 + % *N*/14.14270
Optimum oxygen balance: –28.7%
Volume of explosion gases: 871 L/kg
Heat of explosion (H_2O liq.): 4312 kJ/kg, (H_2O gas): 3991 kJ/kg
Density: 1.67 g/cm^3 by pressing: 1.3 g/cm^3
Lead block test: 370 cm^3/10 g
Impact sensitivity: 3 N·m
Friction sensitivity: up to 353 N
Ashes: not more than 0.4%
Insoluble in acetone: not more than 0.4%
Alkali, as $CaCO_3$: not more than 0.05%
Sulfate, as H_2SO_4: not more than 0.05%
$HgCl_2$: none
Nitrocellulose for gelatinous explosives must gelatinize nitroglycerine completely within 5 min at 60°C
Linters (cotton fibers) as raw material
Properties $(C_6H_{10}O_5)_n$
White fibers
Molecular weight of structural unit: 162.14
Specifications: cellulose content (insoluble in 17.5% NaOH): at least 96%

(*continued*)

Table 2.12 (continued) Characteristics and Specifications of Nitrocellulose

Fat; resin (soluble in CH_2C_{l2}): not more than 0.2%
Optimum moisture: not more than 7.0%
Optimum ash content: not more than 0.4%

Note: See USEPA (2010e), Meyer et al. (2002), ATF (2010).

2.4.14 Nitroglycerin

Nitroglycerin (CAS number 55-63-0) is an oily, colorless liquid, and a high explosive that is so unstable that the slightest jolt, impact, or friction can cause it to spontaneously detonate. Because the molecule contains oxygen, nitrogen, and carbon, when it explodes a large energy is released and its rate of decomposition reaction makes it such a violent explosive that it forms new molecules as depicted in the following chemical equation:

$$4C_3H_5N_3O_9(s) \rightarrow 6N_2(g) + 12CO(g) + 10H_2O\,(g) + 7O_2(g)$$

High explosives are decomposed instantaneously by a supersonic shock wave passing through the material. Based on the chemical equation, 4 mol of nitroglycerin generates 35 mol of hot gases, which makes it one of the most powerful explosives. The characteristics and specifications of nitroglycerin are provided in Table 2.13.

2.4.15 Octagen (HMX)

Octagen, or *octahydro-1,3,5,7-tetranitro-1,3,5,7-tetrazocine* (HMX), is a powerful and relatively insensitive *nitroamine* high explosive, chemically related to RDX. Octagen is insoluble in water and is made by the nitration of hexamine with ammonium nitrate and nitric acid in an acetic acid. It can be used to manufacture *cyclotrimethylene-trinitramine* (RDX), another high explosive similar in structure to HMX. The characteristics and specifications of HMX are shown in Table 2.14.

2.4.16 Pentaerythritol Tetranitrate

PETN is an explosive with high brisance; is very stable; is insoluble in water; is sparingly soluble in alcohol, ether, and benzene; and is soluble in acetone and methyl acetate. Pentaerythrol is mixed into concentrated nitric acid with efficient stirring and cooling to produce PETN. An approximate optimum fraction of 70% HNO_3 should be attained to precipitate the remainder of the product, then acetone is used to finish the product. PETN is more complex to detonate than TNT but it has higher levels of shock and friction sensitivity; explosion will not be produced by

Table 2.13 Characteristics and Specifications of Nitroglycerin

Color: Yellow oil	
CAS number: 55-63-0	
Empirical formula: $C_3H_5N_3O_9$	
Molecular weight: 227.1	
Energy of formation: –1539.8 kJ/kg	
Enthalpy of formation: –1632.4 kJ/kg	
Optimum oxygen balance: +3.5%	
Optimum nitrogen content: 18.50%	
Volume of explosion gases: 716 L/kg	
Heat of explosion	
(H_2O liquid): 6671 kJ/kg	
(H_2O gas): 6214 kJ/kg	
Specific energy: 1045 kJ/kg	
Density: 1.591 g/cm^3	
Solidification point: +13.2°C (stable modification),+2.2°C (unstable modification)	
Specific heat: 1.3 kJ/kg	
Lead block test: 520 cm^3/10 g	
Detonation velocity, confined: 7600 m/s	
Impact sensitivity: 0.2 N·m	
Friction sensitivity: up to 353 N	
Nitroglycerine as a component of explosives	
Nitrogen content	Not less than 18.38%
Abel test at 82.2°C	Not less than 10 min
Glycerol as a raw material	
Smell	Not offensive; pungent
Color	Clear, as pale as possible

(*continued*)

Table 2.13 (continued) Characteristics and Specifications of Nitroglycerin

Reaction to litmus	Neutral
$AgNO_3$ test: traces only	Fatty acids: traces only
Ash content: maximum 0.03%	Water content: maximum 0.50%
Refractive index (*nD*)	20: 1.4707–1.4735
Acidity: not more than 0.3 mL n/10	NaOH/100 mL
Alkalinity: not more than 0.3 mL n/10	HCl/100 mL

Note: See USEPA (2010e,f), Meyer et al. (2002), ATF (2010).

dropping or igniting. Deflagration to detonation transition can take place in some cases. PETN is used to avoid the need for primary explosives; the energy needed for an immediate initiation of PETN by an electric spark is approximately up to 60 mJ. It is a major ingredient of the plastic explosive *semtex*. PETN can only become a violent explosive when it is mixed with other explosives. The explosive that almost brought down the Northwest Airlines flight 253 was extremely powerful, allowing terrorists to use only small quantities to cause enormous damage. PETN crystals are hard to detect if carried in a sealed container. The characteristics and specifications are shown in Table 2.15.

2.4.17 Picric Acid

2,4,6-Trinitrophenol (TNP) is commonly known as *picric acid*; it is soluble in hot water, alcohol, ether, benzene, and acetone. Also, it is highly explosive compared to TNT. It is generated by dissolving phenol during nitration of the resulting *phenoldisulfonic acid* with nitric acid. The crude product is purified by washing with water and needs an elevated pouring temperature. But the solidification point can be reduced by using *nitronaphthalene* or *dinitrobenzene*. The characteristics and specifications of picric acid are presented in Table 2.16.

2.4.18 Plastic Explosives

Plastic explosives (e.g., gelignite, composition 4 or C-4, and plastrite) are commonly called semtex, and they contain high-brisance crystalline explosives, such as octagen and RDX with petroleum jelly (Vaseline) or gelatinized liquid nitro compounds in poly-additive plastics (e.g., polysulfides, polybutadiene, acrylic acid).

Table 2.14 Characteristics and Specifications of HMX

Color: Colorless crystals
CAS number: 2691-41-0
Empirical formula: $C_4H_8N_8O_8$
Molecular weight: 296.2
Energy of formation: +353.6 kJ/kg
Enthalpy of formation: +60.5 kcal/kg = +253.3 kJ/kg
Optimum oxygen balance: –21.6%
Optimum nitrogen content: 37.83%
Volume of explosion gases: 902 L/kg
Heat of explosion (H_2O gas): 5249 kJ/kg, (H_2O liquid): 5599 kJ/kg
Specific energy: 1367 kJ/kg
Density:
α-modification: 1.87 g/cm^3
β-modification: 1.96 g/cm^3
γ-modification: 1.82 g/cm^3
δ-modification: 1.78 g/cm^3
Melting point: 275°C
Modification transition temperatures:
α → ™: 193°C–201°C
β → ™: 167°C–183°C
γ → ™: 167°C–182°C
α→ ®: 116°C
β → ©: 154°C
Transition enthalpies:
α→ ™: 25.0 kJ/kg
β → ™: 33.1 kJ/kg
γ → ™: 9.46 kJ/kg

(*continued*)

Table 2.14 (continued) Characteristics and Specifications of HMX

β → ©: 23.6 kJ/kg	
α → ©: 15.5 kJ/kg	
α → ®: 8.04 kJ/kg	
Specific heat, ®-modification:	
0.3 kcal/kg at 80°C	
Lead block test: 480 cm^3/10 g	
Detonation velocity, confined, ®-modification: 9100 m/s	
Deflagration point: 287°C	
Impact sensitivity: 7.4 N·m	
Friction sensitivity: At 120 N	
Grade A	Not less than 93%
Grade B	Not less than 98%
Melting point	Not less than 270°C
Acetone-insoluble	Not more than 0.05%
Ashes	Not more than 0.03%
Acidity, as CH_3COOH	Not more than 0.02%

Note: See Gibbs and Poppolato (1980), Meyer et al. (2002), ATF (2010), Akhavan (2004).

2.4.19 2,4,6-Trinitrotoluene

2,4,6-Trinitrotoluene is a yellow, odorless solid and is commonly known as TNT; it is usually used in military bombs and grenades, for industrial uses, and in underwater blasting. The production of TNT in the United States occurs solely at military arsenals. Table 2.17 defines the specifications and characteristics of TNT. It is produced by nitration of toluene in several steps. The trinitration step needs highly concentrated mixed acids with free SO_3. The purity grade of the product is determined by its solidification point. TNT is the most important explosive for blasting charges of all weapons used in the military. It is very stable, neutral, and does not attack metals. It can be produced pure and mixed with ammonium nitrate, with aluminum powder, with RDX, and in other combinations.

Table 2.15 Characteristics of PETN

Color: Colorless crystals
CAS number: 78-11-5
Empirical formula: $C_5H_8N_4O_{12}$
Molecular weight: 316.1
Energy of formation: –1,610.7 kJ/kg
Enthalpy of formation: –1,704.7 kJ/kg
Optimum oxygen balance: –10.1%
Optimum nitrogen content: 17.72%
Volume of explosion gases: 780 L/kg
Heat of explosion (H_2O gas): 5,850 kJ/kg, (H_2O liquid): 6,306 kJ/kg
Heat of detonation (H_2O liquid) 6,322 kJ/kg
Specific energy: 1,205 kJ/kg
Density: 1.76 g/cm^3
Melting point: 141.3°C
Heat of fusion: 152 kJ/kg
Specific heat: 1.09 kJ/kg
Lead block test: 523 cm^3/10 g
Detonation velocity, confined: 8,400 m/s = 27,600 ft/s at ρ = 1.7 g/cm^3
Deflagration point: 202°C = 396°F
Impact sensitivity: 3 N·m
Friction sensitivity: 60 N

Note: See Lee and Jaw (2008), Meyer et al. (2002), ATF (2010), Akhavan (2004).

Table 2.16 Characteristics and Specifications of Picric Acid

Color: Yellow crystals
CAS number: 88-89-1
Empirical formula: $C_6H_3N_3O_7$
Molecular weight: 229.1
Energy of formation: –1014.5 kJ/kg
Enthalpy of formation: –1084.8 kJ/kg
Detonation velocity: 7350 m/s at a density of 1.7 g/cm^3
Deflagration point: 570°F
Solidification point: not less than 240°F
Moisture content: not more than 0.1%
Benzene-insoluble: not more than 0.15%
Ash content: not more than 0.1%
Lead content: not more than 0.0004%
Optimum oxygen balance: –45.4%
Iron content: not more than 0.005%
Insolubility in water: not more than 0.15%
Optimum nitrogen content: 18.34%
Volume of explosion gases: 826 L/kg
Heat of explosion(H_2O gas): 3437 kJ/kg, (H_2O liquid): 3350 kJ/kg
Specific energy: 995 kJ/kg
Density: 1.76 g/cm^3
Heat of fusion: 76.2 kJ/kg
Impact sensitivity: 7.4 N·m
Friction sensitivity: 353 N
Specific heat: 1.065 kJ/kg

Note: See US Naval Technical Mission to Japan (1945), Meyer et al. (2002), ATF (2010), Akhavan (2004).

Table 2.17 Characteristics and Specifications of TNT

Color: pale yellow crystals; flakes if granulated
CAS number: 118-96-7
Empirical formula: $C_7H_5N_3O_6$
Molecular weight: 227.1
Energy of formation: –219.0 kJ/kg
Enthalpy of formation: –295.3 kJ/kg
Optimum oxygen balance: –73.9%
Optimum nitrogen content: 18.50%
Volume of explosion gases: 825 L/kg
Heat of explosion: (H_2O gas): 3646 kJ/kg,(H_2O liquid): 4564 kJ/kg
Specific energy: 92.6 mt/kg = 908 kJ/kg
Density, crystals: 1.654 g/cm^3
Density, molten: 1.47 g/cm^3
Solidification point: 80.8°C
Heat of fusion: 96.6 kJ/kg
Specific heat at 20°C: 1.38 kJ/kg
Lead block test: 300 cm^3/10 g
Detonation velocity, confined: 6900 m/s
Deflagration point: 300°C
Impact sensitivity: 1.515 N·m
Friction sensitivity: Up to 353 N

Note: See USEPA (2010e,f), ATF (2010), Akhavan (2004), US Naval Technical Mission to Japan (1945).

2.5 Mechanical Components and Applications of Chemical Explosives

There have been almost constant bomb threats after the Boston Marathon explosions in April 2013. The general public should learn to recognize potential home-made explosives to prevent public injury or disaster. Terrorists and self-radicalized individuals aim to inflict mass injuries, casualties, and property damage, and chemical

explosives are typically their first weapons of choice. Some of the common mechanical components and considerations to explosives are presented in Sections 2.5.1 through 2.5.17.

2.5.1 Alginates

Alginates are anionic polysaccharides that are capable of binding 200–300 times their own volume of water. They can be used as swelling agents to explosive mixtures in order to improve the resistance of such explosives to moisture.

2.5.2 Aluminum Powder

Aluminum powder is usually a crucial ingredient in explosives for producing heat explosion, and as a result a higher temperature is generated in the fumes. If the proportion of aluminum in the explosive formulation is extremely high, a gas impact effect results, as successive contact of the unreactive parts of the fumes with atmospheric oxygen may produce a delayed second explosion.

2.5.3 Base Charge

The base charge is normally the finishing component of any blasting detonator. It is composed of a secondary nitramine explosive (Ledgard 2002).

2.5.4 Blasting Caps

Blasting caps are made of cylindrical copper or aluminum capsules, which are utilized as initiators of explosive charges. PETN or other types of secondary charge is added to achieve a higher brisance. A blasting cap can be ignited by the flame of a safety fuse or electrically. The normal size should only be used with slow fuses. Currently, the number 8 blasting cap is commercially available for all practical purposes. The number 8 blasting cap consists of a 300 mg primary charge and an 800 mg secondary charge, and is 0.4–5 cm in length and 0.7 cm in external diameter.

2.5.5 Blasting Galvanometer

A blasting galvanometer is an instrument that is used for testing electric blasting circuits, enabling the blaster to locate breaks, short circuits, or faulty connections before an attempt is made to fire the shot.

2.5.6 Blasting Machine

Two blasting machines exist: (1) one with direct energy supply equipped with a self-induction or a permanent magnet generator, which is made to rotate with the

aid of a twist knob, impact knob, or spring extension; and (2) one with an indirect energy supply, in which the generated electrical energy is stored in a capacitor and, after the discharge voltage has been attained, the breakthrough pulse is sent to a blasting train. In order to ignite *bridgewire detonators*, they need to be installed and connected in parallel; thus, the output of the machines will be higher as more than 95% of the electrical energy is lost in the blasting circuit. Special powerful machines are required to set off highly insensitive detonators for blasting carried out in high mountainous areas and in other locations endangered by high-voltage induction; a very strong priming pulse must be applied in such cases.

2.5.7 Blast Meters and Boosters

Blast meters are simple devices used to determine the maximum pressure of a shock wave. They consist of steel bodies into which holes of different diameters are drilled and covered with aluminum foil. The smallest diameter is determined at which the foil covering is penetrated. The device can be calibrated by static pressure. A booster can be a cap-sensitive cartridge or a press-molded cylinder for the initiation of non-cap-sensitive charges, such as blasting agents or cast TNT. A booster is, in rocketry, a rocket device that accelerates the missile to attain the required speed after the start.

2.5.8 Bridgewire Detonator

Bridgewire detonators are used in the industrial detonation of explosive charges. They contain a bridge made of thin resistance wire with an igniting pill built around the wire and immersed in pyrotechnical substance after drying, which will glow by using electric pulse. The delayed-action detonators may be set for a delay of half a second (half-second detonators) or for a delay of 2–34 ms (millisecond detonators). Hence, if multiple charges are to be detonated at the same time, the detonators should be connected in series with the connecting wire. Special blasting machines must be used in parallel connection of detonators.

2.5.9 Brisance

Brisance is the destructive fragmentation effect of a charge on its designated and direct vicinity. The relevant parameters of explosives are detonation rate, loading density, gas yield, and heat of explosion. The higher the loading density of the explosive, the higher is the speed of the reaction rate and the intensity of the impact of the detonation. Moreover, an increase in density is in conjunction with an increase in the detonation rate of the explosive, whereas the shock wave pressure in the detonation front varies with the square of the detonation rate. Therefore, a higher loading density could be a very significant factor.

2.5.10 Deflagration

Deflagration is a technical term describing subsonic combustion that usually propagates through the liberated heat of reaction. The burning of powder is a deflagration process.

2.5.11 Delay Time and Element

Delay time is the time or interval between the instant a device carrying the fuze is launched and the instant the fuze becomes armed. Delay compositions are mixtures of substances that when pressed into delay tubes react without the progression of gaseous products and thus ensure minimum variation in the delay period. Examples of such mixtures are potassium permanganate with antimony, and redox reactions with fluorides and other halides. The delay element can be an explosive train component consisting of a primer, a delay column, and a relay detonator or transfer charge collected in that order in a single housing to produce a regulated time interval. Hence, the time or interval between the initiation of the fuze and the detonation can be set.

2.5.12 Detonation

Detonation is a chemical reaction created by an explosive agent/material which produces a shock wave. Increases in temperature and pressure gradients are created in the wave front in order to initiate the chemical reaction instantaneously. Detonation speeds may be in the approximate range of 1500–9000 m/s; slower reactions, which are propagated by thermal conduction and radiation, are known as deflagration.

2.5.12.1 Shock Wave

Shock waves are generated in nonexplosive form by a rapid change in pressure. Allow a movable piston in a tube to be suddenly accelerated from rest and then continue its motion at a constant rate. The air in front of the piston will be compressed and warms up a little; the compression range is determined by the velocity of sound in the air. In addition, allow the piston to accelerate again and continue its motion at a higher rate. The new compression is applied to the medium, part of which is already in motion; it now moves at a quicker rate, the movement of the subject is superposed, and the sonic velocity is intensified in a warmer medium. If the medium is an explosive gas mixture rather than air, an explosive reaction will be instantly initiated in front of the shock wave. Explosions normally produce a shock wave in the surrounding air. Hence, this compression shock is the standard principle of the long-distance effect of explosions. According to Meyer et al. (2002), if the propagation of the shock wave is nearly spherical, the compression ratio p_1/p_0

decreases rapidly, and so does the p_0 velocity of matter W; it becomes zero when the shock wave becomes an ordinary sound wave. If the explosion-generated shock wave is propagated in three-dimensional space, its effect decreases with the third power of the distance. This is the guideline adopted by German accident prevention regulations, in which the safety distance (in meters) is quantified by the term $f \cdot \sqrt[3]{M}$, where M is the maximum amount of explosives, in kilograms, which is present in the building or asset at any time, while f is a factor that varies, according to the required degree of safety, from 1.5 to 8 (distance from the nondangerous part of an asset). This expression can be used to design the location of an emergency response station for a major asset, to immediately respond in the event of a terrorist attack as illustrated in the scenarios in combat zones presented in Chapter 7. Meanwhile, Meyer et al. (2002) pointed out that the shock wave theory is easier to understand if we consider a planar shock wave, on the assumption that the tube is indestructible (such shock wave tubes are utilized as research instruments in gas dynamics and in solid-state physics; the shock sources are explosions or membranes bursting under pressure). Comparative treatment of the behavior of the gas in the tube yields the following relationships.

From the law of conservation of mass,

$$\rho_0 D = \rho_1 (D - W) \quad \text{or} \quad v_1 D = v_0 (D - W) \tag{2.1}$$

From the law of conservation of momentum,

$$p_1 - p_0 = \rho_0 DW \quad \text{or} \quad v_0 (p_1 - p_0) = DW \tag{2.2}$$

From the law of conservation of energy,

$$p_1 W = \eta_0 D \left(\frac{e_1 - e_2 + W^2}{2} \right) \tag{2.3}$$

Rearrangements yield the so-called *Hugoniot* equation:

$$e_1 - e_0 = \frac{1}{2} (p_1 + p_0)(v_0 - v_1) \tag{2.4}$$

The following expressions are obtained for velocity D of the shock wave and for the velocity of matter W:

$$D = v_0 \sqrt{\frac{\rho_1 - \rho_0}{v_0 - v_1}} \tag{2.5}$$

and

$$W = \sqrt{(p_1 - p_0)(v_0 - v_1)} \tag{2.6}$$

These relationships are valid irrespective of the state of aggregation.

2.5.12.2 Detonation Wave Theory

An explosive chemical reaction produced in the wave front because of the extreme temperature and pressure conditions is called a detonation wave. The development and transmission of the shock wave is sustained by the energy of the reaction. The equations presented in Section 2.5.12.1 are still valid; the equation parameters represent the following:

p_1—detonation pressure
ρ_1—density of gaseous products in the front of the shock wave; this density is thus higher than the density of the explosive α_0
D—detonation rate
W—velocity of fumes
Equation 2.1 remains unchanged

As p_0 is negligibly small compared to the detonation pressure p_1, we can write Equation 2.2 as $p_1 = \rho_0 DW$.

The pressure created by detonation in the wave front is proportional to the product of density, detonation rate, and fume velocity, given that fume velocity is the square of the detonation rate. For a known explosive, the detonation velocity increases with increasing density. As per the equation $p_1 = \rho_0 DW$, the detonation pressure increases noticeably if the initial density of the explosive substance can be raised to its optimum charge, for example, by casting or pressing, or if the density of the explosive substance is elevated (e.g., the density of TNT is 1.64 and that of octogen is 1.96). High density of the explosive is important if high W brisance is required. Meanwhile, the detonation pressure and rate may be reduced by decreasing α_0, that is, by the application of a more loosely textured explosive material. This is initiated and employed if the blasting has to be done on softer rocks and if a weaker *thrust* effect is expected.

The determination of the maximum level of detonation pressure p_1, in Equation 2.7, has been studied by x-ray measurements. While the detonation velocity can be quantified by electronic recorders, there is no standard quantification for the fume velocity W; but it can be projected by the direction of angle of the fumes behind the wave front. The relation between D and W is $W = D/\gamma + 1; \gamma$ is presented as the *polytrop exponent* in the modified state equation:

$$p = C\rho^{\gamma}, \text{ while } C = \text{constant}$$

The value of (γ) is nearly 3; therefore, p_1 is

$$p_1 = \frac{\eta_0 D^2}{4} \tag{2.7}$$

Equation 2.2 can be recomputed as

$$p_1 - p_2(v_0 - v_1)\rho_0^2 D^2 \tag{2.8}$$

Equation 2.4, utilized in the detonation development relating the chemical energy of reaction q, becomes

$$e_1 - e_0 = \frac{1}{2}(p_1 + p_0)(v_0 + v_1) + q \tag{2.9}$$

Equations 2.5 and 2.6 remain unmodified, but D is currently equivalent to the detonation rate, whereas W represents the fume velocity.

2.5.12.3 Selective Detonation

Selectivity in the course of a detonation process is noted when processes with very different sensitivities, and thus also with very different induction periods, participate in the intensive chemical reaction produced by the shock wave (Ahrens 1977). If the concentration or the amount of the shock wave is minimal as a result of external conditions—an explosion in an unconfined space, for example—the induction periods of less-sensitive reactions may become infinite, that is, the reaction may fail to take place. Hence, this selectivity is important for ion exchanges. According to Meyer et al. (2002), if the explosive is detonated while it is unconfined, the only reaction that will occur is that of the nitroglycerine–nitroglycol mixture, which is fast and limited by its relative proportion and is thus firedamp safe.

2.5.12.4 Sympathetic Detonation

Sympathetic detonation signifies the beginning of an explosive charge without a priming mechanism by the detonation of another charge. The maximum distance between two cartridges in line is based on the flashover tests, by which the detonation is transmitted. The transmission method is complicated by shock wave, hot reaction products, and even the *hollow charge* effect. The detonation velocity is defined as the rate of propagation of a detonation in an explosive; if the density of the explosive is at its optimum charge and if the explosive is charged into columns that are considerably wider than the critical diameter, the detonation velocity is a characteristic of each individual explosive.

2.5.12.5 Detonation Development Distance

Detonation development distance is a term denoting the distance or space required for the full detonation rate to be attained. In initiating explosives, this distance is short. The detonation development distance relating to less sensitive explosive materials is strongly influenced by the consistency, density, and cross section of the charge.

2.5.13 Electroexplosive Device

An electroexplosive device (EED) is a detonator or initiator initiated by an electric current. A *one-ampere/one-watt initiator* or EED is one that will not fire when 1 A of current at 1 W of power is delivered and given to a bridgewire for a designated time.

2.5.14 Oxidizer and Oxygen Balance of Explosives

All explosive materials contain and require oxygen to achieve an explosive reaction. In addition, oxygen can be introduced by *nitration*. The most critical solid-state oxidizers are nitrates, particularly ammonium nitrate and sodium nitrate for explosives. The quantity of oxygen, released as a result of total conversion of the explosive material to CO_2, H_2O, SO_2, Al_2O_3, etc., is called *positive* oxygen balance. If the amount of oxygen is insufficient, which is known as a *negative* oxygen balance, the deficient amount of the oxygen needed to complete the reaction is designated with a negative sign. The most favorable composition for an explosive can be easily quantified from the oxygen values of its components. Commercial explosives must have an oxygen balance close to zero in order to minimize the production of toxic gases such as monoxide, as well as nitrous gases.

2.5.15 Heat of Explosion

The heat of explosion may be calculated using theoretical principles and experimentally determined. The quantified value is the difference between the energies of formation of the explosive components and the energies of formation of the explosion products. Moreover, the values of heat of explosion can be quantified from the *partial* heat of explosion of the components of the propellant. The calculated values do not agree exactly with those obtained by experiment; if the explosion takes place in a bomb, the true compositions of the explosion products are different and, moreover, vary with the loading density. In accurate calculations, these factors must be taken into consideration.

2.5.16 Underwater Detonation

Destructive effects of underwater detonation change according to distance and closeness effects. The first effect is caused by the action of the pressure shock wave

and the latter mainly by the thrust created by the increasing and intensifying gas bubble. Underwater detonation can severely damage underwater tunnels.

2.5.16.1 Shock Wave of Underwater Detonation

The adjacent layer of water is compressed under the effect of high pressure, which transmits that pressure onto the next level, and this transfers the pressure onto further levels or a chain reaction to different levels. The velocity of propagation intensifies with pressure, accordingly generating a steeply ascending pressure front, which reveals the characteristic of a shock wave to the pressure wave. At the beginning, the velocity of propagation surpasses that of the speed of sound, but the velocity declines with greater distance. Thus, the optimum pressure is directly proportional to the cube root of the charge weight and inversely proportional to the distance or space, as depicted in the following expression:

$$P_{max} = \frac{CL^{1/3}}{e}$$

where

P is pressure in bar
L is loading weight in kilograms
e is the distance in meters
C is the typical empirical factor of 500

Underwater detonation can damage an underwater tunnel (immersed tunnel).

2.5.16.2 Gas Bubble

An underwater explosion is created by the gas that primarily penetrates the small cavity formerly filled by an explosive, thus creating a gas bubble under a high level of pressure, which then expands. Accordingly, the bubble expansion creates the water mass to progress radially at high velocity away from the point of explosion known as *thrust*. The optimum amount of kinetic energy distributed to the water during an explosion is called *thrust energy*. The gas bubble can be oscillated repeatedly several times and is forced upward toward the surface of the water. The variation in pressure between the top and the bottom layers of the bubble creates the bottom layer to move at a higher velocity, propelling it upward into the bubble. It is likely for both surfaces to meet. Within a partial area, the water obtains an upward thrust, producing a *water hammer*. Effective and powerful underwater explosives with mixtures of aluminum powder are those that can generate a high-pressure gas bubble for the formation of the thrust. Detection technologies may need to be developed for detecting the chemical components of explosives that generate a high-pressure gas bubble upon entry into major water assets.

2.5.17 Calculation of Explosives

One way to calculate the total quantity of explosives recommended by Langefors and Khilstrom (1963) is

$$Q = 0.07B^2 + 0.4B^3 + 0.004B^4$$

where

B is the burden in meters
Q is the quantity of explosive in kilograms

The first term is the explosive needed to produce the surface blast design and to satisfy other dissipative processes. The second term is the principal term that relates the weight of the explosive and the weight of rock. The third term, usually very small, provides the energy for the swelling and lifting of the mass.

2.5.18 Hazards of Explosives

High explosives are capable of severely mutilating the human body. Explosives tend to rip the body into different pieces like a shark with jagged uneven bits of body parts removed. According to Jared Ledgard (2002), other than the obvious effects of injuries caused by explosives upon the body, there are effects known as the secondary effects of exposure to detonations which include temporary loss of vision, hearing impairment, fragmentation wounds, burns, and inhalation and/or skin absorption of poisonous fumes. Fragmentation wounds cause a whole multitude of problems as they are like multiple gunshot wounds. Patients have died many hours later due to many types of complications arising from fragmentation wounds.

2.6 Chemical Threats as Poisonous Weapons and Lethal Dose (LD_{50})

Chemical threats are characterized by the rapid onset of medical symptoms and easily observed signatures such as colored residue, dead foliage, pungent odor, and dead insect and animal life based on the US Central Intelligence Agency (CIA). Some of the common chemical terms are enumerated in Table 2.18.

Terrorists take into consideration a wide range of toxic chemicals for attacks. Typical plots focus on poisoning foods or spreading an agent on surfaces to poison through skin contact, but some also include broader dissemination techniques. Meanwhile, this book focuses on cyanide (CN) and arsenic compounds used for WMD through water supply contamination as practical examples; the chemical threats from CIA guidelines are also listed below as part of the literature research.

Table 2.18 Chemical Terms

Chemical Terms	*Description*
Acetylcholinesterase (CAS no. 9000-81-1)	An enzyme that hydrolyzes the neurotransmitter acetylcholine. The action of this enzyme is inhibited by nerve agents.
Aerosol (CAS no. 577-11-7)	Fine liquid or solid particles suspended in a gas (e.g., fog or smoke).
Atropine (CAS no. 51-55-8)	A compound used as an antidote for nerve agents. It is tropane alkaloid derived from nightshade (*Atropa belladonna*), Jimson weed (*Datura stramounium*), and mandrake (*Mendragora officinarum*).
Toxic agents (cancer-causing agents or agents causing immediate death; see Tables 2.19 through 2.23)	Produce incapacitation, serious injury, or death. They can be used to incapacitate or kill victims. These agents are the choking, blister, nerve, and blood agents.
Choking agents a. Ammonia (CAS no. 7664-41-7) b. Bromine (CAS no. 7726-95-6) c. Chlorine (CAS no. 7782-50-5) d. Hydrogen chloride (CAS no. 7647-01-0) e. Methyl bromide (CAS no. 74-83-9) f. Methyl isocyanate (CAS no. 624-83-9) g. Osmium tetroxide (CAS no. 7440-04-2) h. Disphosgene (CAS no. 503-38-8) i. Phosgene (CAS no. 75-44-5) j. Phosphine (CAS no. 7803-51-2) k. Phosphorus (CAS no. 7723-14-0) l. Sulfuryl fluoride (CAS no. 7791-25-5)	Substances that cause physical injury to the lungs. Exposure is through inhalation. In extreme cases, membranes swell and lungs become filled with liquid. Death results from lack of oxygen.

(*continued*)

Table 2.18 (continued) Chemical Terms

Chemical Terms	*Description*
Blister agents a. Lewisite (CAS no. 40334-69-8) b. Nitrogen mustard (CAS no. 538-07-8) c. Phosgene oxime (CAS no. 1794-86-1) d. Sulfur mustard (CAS no. 505-60-2)	Substances that cause blistering of the skin. Exposure is through liquid or vapor contact with any exposed tissue (eyes, skin, and lungs).
Nerve agents a. Sarin (CAS no. 107-44-8) b. Soman (CAS no. 96-64-0) c. Tabun (CAS no. 77-81-6) d. VX (CAS no. 50782-69-9) e. Cyclosarin (CAS no. 74192-15-7)	Substances that interfere with the central nervous system. Exposure is primarily through contact with the liquid (skin and eyes) and secondarily through inhalation of the vapor. Three distinct symptoms associated with nerve agents are pin-point pupils, an extreme headache, and severe tightness in the chest.
Blood agents a. Arsine (CAS no. 7784-42-1) b. Carbon monoxide (CAS no. 630-08-0) c. Cyanogen chloride (CAS no. 506-77-4) d. Hydrogen cyanide (CAS no. 74-90-8) e. Potassium cyanide (CAS no. 1511-50-8) f. Sodium cyanide (CAS no. 143-33-9)	Substances that injure a person by interfering with cell respiration.
Chemical agent	A chemical substance that is intended for use in military operations to kill, seriously injure, or incapacitate people through its physiological effects. The agent may appear as a vapor, aerosol, or liquid; it can be either a casualty/toxic agent or an incapacitating agent.
Cutaneous	Pertaining to the skin.

Table 2.18 (continued) Chemical Terms

Chemical Terms	*Description*
Decontamination	The process of making any person, object, or area safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.
G-series nerve agents	Chemical agents of moderate to high toxicity developed in the 1930s. Examples are tabun (GA), sarin (GB), and soman (GD).
Incapacitating agents a. 3-Quinuclidinyl benzilate (BZ) (CAS no. 6581-06-2) b. Fentanyl (CAS no. 990-73-8) c. Etorphine (CAS no. 14521-96-1)	Produce temporary physiological and/or mental effects through action on the central nervous system. Effects may persist for hours or days, but victims usually do not require medical treatment. However, such treatment speeds recovery.
Vomiting agents a. Diphenylchlorarsine (CAS no. 14521-96-1) b. Diphenylcyanoarsine (CAS no. 23525-22-6) c. Diphenylaminearsine (CAS no. 578-94-9)	Produce nausea and vomiting effects, can also cause coughing, sneezing, pain in the nose and throat, nasal discharge, and tears.
Tear agents	Produce irritating or disabling effects that rapidly disappear within minutes after exposure ceases.
Central nervous system depressants	Compounds that have the predominant effect of depressing or blocking the activity of the central nervous system. The primary mental effects include the disruption of the ability to think, sedation, and lack of motivation.
Central nervous system stimulants a. Mixed amphetamine salts (CAS no. 51-64-9 and 300-62-9) b. Dextroamphetamine (CAS no. 300-62-9) c. Methylphenidate (CAS no. 113-45-1) d. Pemoline (CAS no. 2152-34-3)	Compounds that have the predominant effect of flooding the brain with too much information. The primary mental effect is loss of concentration, causing indecisiveness and the inability to act in a sustained, purposeful manner.

(*continued*)

Table 2.18 (continued) Chemical Terms

Chemical Terms	*Description*
Industrial agents	Chemicals developed or manufactured for use in industrial operations or research by industry, government, or academia. These chemicals are not primarily manufactured for the specific purpose of producing human casualties or rendering equipment, facilities, or areas dangerous for use by man. HCN, cyanogen chloride, phosgene, chloropicrin, and many herbicides and pesticides are industrial chemicals that can also be chemical agents.
Liquid agent	A chemical agent that appears to be an oily film or droplets. The color ranges from clear to brownish amber.
Nonpersistent agent	An agent that on release loses its ability to cause casualties after 10–15 min. It has a high evaporation rate and is lighter than air and disperses rapidly. It is considered to be a short-term hazard. However, in small unventilated areas, the agent will be more persistent.
Organophosphorous compound	A compound containing the elements phosphorus and carbon whose physiological effects include inhibition of acetylcholinesterase. Many pesticides (malathione and parathion) and virtually all nerve agents are organophosphorous compounds.
Percutaneous agent	Able to be absorbed by the body through the skin.
Persistent agent	An agent that on release retains its casualty-producing effects for an extended period of time, usually anywhere from 30 min to several days. A persistent agent usually has a low evaporation rate, and its vapor is heavier than air.

Table 2.18 (continued) Chemical Terms

Chemical Terms	*Description*
	Therefore, its vapor cloud tends to hug the ground. It is considered to be a long-term hazard. Although inhalation hazards are still a concern, extreme caution should be taken to avoid skin contact as well.
V-series nerve agents	Chemical agents of moderate to high toxicity developed in the 1950s. They are generally persistent. Examples are VE, VG, VM, VS, and VX.
Vapor agent	A gaseous form of a chemical agent. If heavier than air, the cloud will be close to the ground. If lighter than air, the cloud will rise and disperse more quickly.

Sources: Data from US Central Intelligence Agency, Terrorist CBRN: Materials and effects, https://www.cia.gov/library/reports/general-reports-1/cbr_handbook/cbrbook.htm#6, accessed October 18, 2010 and January 1, 2013, 1998; US Central Intelligence Agency, Terrorist CBRN: Materials and effects. https://www.cia.gov/library/reports/general-reports-1/terrorist_cbrn/terrorist_CBRN.htm, accessed October 18, 2010 and January 1, 2013, 2010.

Even a relatively inept attack with limited mortality and property damage could accomplish the terrorists' goal of demoralization. Based on the US DoD CBRN (2008), chemical substances that are used in terrorism are intended to kill, seriously injure, or incapacitate humans through their physiological effects. The quantity of chemicals needed for terrorists to generate mass casualties is normally based on the LD_{50} of the chemical or chemical compound. The LD_{50} of the chemical threats are presented herein.

2.6.1 Chemicals' LD_{50}

LD stands for *lethal dose*, and LD_{50} is the amount of chemical(s), given all at once, which causes the death of 50% of a group of test animals. It is a standard quantification and basis of acute toxicity that is stated in milligrams (mg) of chemical or contaminant per kilogram (kg) of body weight. LC stands for *lethal concentration*, and it usually refers to the concentration of a chemical in the atmosphere. Because

of the changeability of *dose–response effects*, the toxicity of a substance is commonly expressed as the concentration or dose that is lethal to 50% of the exposed population (LC_{50} or LD_{50}). It represents the dose required to kill 50% of a population of test animals (e.g., rats, rabbit, mice). Hence, the lower the LD_{50} dose, the more toxic are the contaminants or chemicals, which is the primary basis for the terrorists to succeed in attacking water supply.

2.6.2 Cyanide

Cyanide (CN; CAS no. 57-12-5) can be disseminated as contact poisons when mixed with chemicals that enhance skin penetration. Exposure to CN may produce nausea, vomiting, palpitations, confusion, hyperventilation, anxiety, and vertigo, which may progress to agitation, stupor, coma, and death. At high doses, it causes immediate collapse. CN is an inhibitor of the enzyme *cytochrome c oxidase* in the fourth complex of the electron transport chain, and it is found in the membrane of the mitochondria of eukaryotic cells. CN attaches to the iron within this protein. The binding of CN to this *cytochrome* prevents the transport of electrons from *cytochrome c oxidase* to oxygen. As a result, the electron transport chain is disrupted, meaning that the cell can no longer aerobically produce *adenosine triphosphate* (ATP) for energy. Tissues that mainly depend on aerobic respiration, such as the central nervous system and the heart, are particularly affected. A fatal dose for humans can be as low as 1.5 mg/kg body weight (USEPA 1987). According to the International Program on Chemical Safety (IPCS), sodium cyanide is a highly toxic chemical compound and a deadly human poison by ingestion, and the probable oral LD in humans is less than 5 mg/kg or a taste (less than seven drops) is super toxic for a 70 kg (150 lb) person.

2.6.2.1 Cyanide LD_{50}

The LC_{50} for gaseous hydrogen cyanide (HCN) is 100–300 parts per million (ppm). Inhalation of CN in this range results in death within 10–60 min, with death coming more quickly as the concentration increases. Inhalation of 2000 ppm of HCN causes death within 1 min. The LD_{50} for ingestion is 50–200 mg, or 1–3 mg/kg body weight, calculated as HCN. Meanwhile, for contact with unabraded skin, the LD_{50} is 100 mg/kg body weight with HCN (ICMC 2009). The LD_{50} of sodium cyanide is 6.4 mg/kg (oral rat).

2.6.3 Mustard Agents

According to the US CIA (2010), a mustard agent is a blister agent that poses a contact and vapor hazard. Its color ranges from clear to dark brown depending on purity, and it has characteristic garlic-like odor. Mustard is not commercially

available, but its synthesis does not require significant expertise. In fact, the terrorist enemies of the United States are usually taught how to synthesize this agent. The risk of acute poisoning exists with the use of sulfur mustard vapor in war (IPCS 1996). It can generate a catastrophe by emission within an overpopulated area. It causes damages to the lungs, and death by suffocation in severe cases due to water accumulation in the lungs. The medical treatments are very limited. Cases of leukemia, and lung and stomach cancers were observed in Iranian combatants who were exposed once to sulfur mustard (IPCS 1996). Exposure to super-lethal concentrations may induce convulsions, coma, and death within 1 h after exposure (IPCS 1996).

2.6.4 Nerve Agents

Nerve agents such as sarin, tabun, and VX disrupt a victim's nervous system and cause convulsions that can lead to death. Currently, these agents are not commercially available. Sarin, tabun, and VX are less likely to be used in water supply, but there are commercially available chemicals with similar properties.

2.6.5 Toxic Industrial Agents

There are a wide range of toxic industrial chemicals that are not as toxic as CN, mustard, or nerve agents which can be used in much larger quantities to compensate for their lower toxicity. Moreover, the effects of industrial agents such as chlorine, organophosphate pesticides, and phosgene are similar to those of the mustard agent. According to US CIA (2010), organophosphate pesticides are much less toxic, and their effects and medical treatments are the same as for military-grade nerve agents.

2.6.6 Arsenic

Historically, arsenic (CAS no. 744-38-2) has been used as a poison in wars, agriculture industry, and for household use. There are arsenic-based insecticides, such as control fire ants, that can be used for water poisoning. It appears in group I or class-A human carcinogens in the lists of United States Environmental Protection Agency (USEPA) and International Agency for Research on Cancer (IARC). Moreover, it cannot be easily destroyed. It simply changes its form and moves around in the environment (ODHS 2002). Major uses of arsenic in the United States have been as rodent poisons, insecticides, biocides, and weed killers containing arsenic in both organic and inorganic forms. In pure form, arsenic is a tasteless, odorless white powder or clear crystals. Ingestion of 2 g or more may be lethal in a very short time. Arsenic disrupts ATP production through several mechanisms. ATP is a multifunctional nucleotide that plays an important role in cell biology as

a coenzyme that is the molecular unit of currency of intracellular energy transfer (Knowles 1980). Knowles pointed out that, at the level of the citric acid cycle, arsenic inhibits *pyruvatedehydrogenase*, and by competing with phosphate, it uncouples oxidative phosphorylation, thus inhibiting energy-linked reduction of *nicotinamide adenine dinucleotide* (NAD+), mitochondrial respiration, and ATP synthesis. These metabolic interferences lead to death from multisystem organ failure, probably from necrotic cell death (Klaassen and Watkins 2003).

Arsenic compounds are irritants, systemic toxins, and carcinogens in humans. The trivalent arsenic compounds are the ones that are the most toxic to humans. Initial responses to acute poisoning include burning of the lips, constriction of the throat, and dysphagia (Hathaway et al. 1991). This is followed by excruciating pain in the abdominal region, severe nausea, vomiting, and diarrhea. Toxic effects on the liver, blood-forming organs, both central and peripheral nervous systems, and the cardiovascular system may also occur. Convulsions, coma, and death may follow within 24 h of severe poisoning (Hathaway et al. 1991). Acute inhalation exposures to arsenic compounds may result in damage to the mucous membranes of the respiratory system (Parmeggiani 1983). Severe irritations of the nasal mucosae, larynx, and bronchi have been observed following exposures to arsenic compounds. In addition, exposed skin may become irritated; cases of dermatitis have been reported following dermal contact with arsenic compounds (Parmeggiani 1983). Conjunctivitis, visual disturbances, hyperpigmentation of the skin, and perforation of the nasal septum have been described in the literature (Hathaway et al. 1991). Chronic exposure causes damage to the nervous system, cardiovascular system, and liver (Parmeggiani 1983). Anemia and leukocytopenia have been reported to occur following chronic exposures to arsenic compounds (Parmeggiani 1983). Cancers of the skin, lungs, larynx, lymphoid system, and viscera have been identified as potential responses to arsenic poisoning (Hathaway et al. 1991). IARC has reviewed the available data and considers arsenic to be a Group 1 carcinogen with sufficient evidence of carcinogenicity in humans (IARC 1987).

2.6.6.1 Arsenic LD_{50}

Organic forms of arsenic appear to have a lower toxicity than its inorganic forms. Research has shown that arsenites (trivalent forms) have a higher acute toxicity than arsenates (pentavalent forms) (Kingston et al. 1993). The acute minimal LD of arsenic in adults is estimated to be 70–200 mg or 1 mg/kg/day (Dart 2004).

2.6.7 Inorganic Contaminants

Some of the inorganic chemicals are man-made and some of it occur naturally. Tables 2.19 and 2.20 introduce the health hazards of inorganic chemicals.

Table 2.19 Inorganic Contaminants' Health Effects

Contaminant	*Health Effects*
Antimony (CAS no. 744-36-0)	Antimony has been shown to decrease longevity and alter blood levels of cholesterol and glucose in laboratory animals, such as rats, exposed to high levels during their lifetime.
Asbestos (CAS no. 12172-73-5)	Studies have shown that asbestos has produced lung tumors in laboratory animals. The available information on the risk of developing gastrointestinal tract cancer associated with the ingestion of asbestos from drinking water is limited. Ingestion of intermediate-range chrysotile asbestos fibers greater than 10 μm in length is associated with causing benign tumors in male rats. Chrysotile was the predominant type of asbestos detected in a national survey of the water supplies of 77 communities in North America.
Barium (CAS no. 7440-39-3)	Barium may damage the heart and cardiovascular system and is associated with high blood pressure in laboratory animals, such as rats, exposed to high levels during their lifetime.
Beryllium (CAS no. 7440-41-7)	Beryllium compounds have been associated with damage to the bones and lungs and induction of cancer in laboratory animals such as rats and mice, when the animals are exposed to high levels over their lifetime. Chemicals that cause cancer in laboratory animals may also increase the risk of cancer in humans who are exposed during long periods of time.
Cadmium (CAS no. 7440-43-9)	Cadmium has been shown to damage the kidneys in animals, such as rats and mice, when the animals are exposed to high levels over their lifetime. Some industrial workers who were exposed to relatively large amounts of this chemical during working careers also suffered damage to the kidneys.
Chromium (CAS no. 7440-47-3)	Chromium has been shown to damage the kidneys, nervous system, and the circulatory system of laboratory animals such as rats and mice when the animals are exposed to high levels. Some humans who were exposed to high levels of this chemical suffered liver and kidney damage, dermatitis, and respiratory problems.

(*continued*)

Table 2.19 (continued) Inorganic Contaminants' Health Effects

Contaminant	*Health Effects*
Cyanide	See Section 2.6.2.
Fluoride (CAS no. 7782-41-4)	Exposure to drinking water levels above 4.0 mg/L for many years may result in some cases of crippling skeletal fluorosis, which is a serious bone disorder.
Mercury (CAS no. 7439-97-6)	Mercury has been shown to damage the kidneys of laboratory animals, such as rats, when the animals are exposed to high levels during their lifetime.
Nickel (CAS no. 7440-02-0)	Nickel has been shown to damage the heart and liver in laboratory animals when the animals are exposed to high levels over their lifetime.
Nitrate (CAS no. 14797-55-8)	Excessive levels of nitrate in drinking water have caused serious illness and sometimes death in infants less than 6 months of age. The serious illness in infants is caused because nitrate is converted to nitrite in the body. Nitrite interferes with the oxygen-carrying capacity of the child's blood. This is an acute disease in that symptoms can develop rapidly in infants. In most cases, health deteriorates over a period of days. Symptoms include shortness of breath and blueness of the skin. Clearly, expert medical advice should be sought immediately if these symptoms occur.
Nitrite (CAS no. 14797-65-0)	Although excessive levels of nitrite in drinking water have not been observed, other sources of nitrite have caused serious illness and sometimes death in infants less than 6 months of age. The serious illness in infants is caused because nitrite interferes with the oxygen-carrying capacity of the child's blood. This is an acute disease in that symptoms can develop rapidly. However, in most cases, health deteriorates over a period of days. Symptoms include shortness of breath and blueness of the skin. Clearly, expert medical advice should be sought immediately if these symptoms occur.
Selenium (CAS no. 7782-49-2)	In humans, exposure to high levels of selenium over a long period of time has resulted in a number of adverse health effects, including a loss of feeling and control in the arms and legs.

Table 2.19 (continued) Inorganic Contaminants' Health Effects

Contaminant	*Health Effects*
Thallium (CAS no. 7440-28-0)	This chemical has been shown to damage the kidneys, liver, brain, and intestines of laboratory animals when the animals are exposed to high levels during their lifetime.

Note: See ATSDR (2010a), California EPA-OEHHA (2010), MSDS (2010), Oxford University (2010), USEPA (2010a,c).

2.6.8 Organic Contaminants

Organic compounds are chemicals that are constructed from molecules that possess carbon-based atoms. Many organic liquid compounds are characterized as immiscible or have a very low solubility in water. Nonaqueous phase liquids (NAPLs) are hydrocarbons that exist as a separate, immiscible phase when in contact with water. Differences in the physical and chemical properties of water and NAPL result in the formation of a physical interface between the liquids, which prevents the two fluids from mixing with each other. NAPLs are typically classified as either light LNAPLs (e.g., petroleum products) that have densities less than that of water or dense nonaqueous phase liquids (DNAPLs; e.g., chlorinated solvents) that have densities greater than that of water. Refined petroleum products are generally complex mixtures of a variety of organic compounds with minor fractions of organic and inorganic additives that fall into a number of chemical classes. Chlorinated solvents are generally released to the environment in a more or less pure form as opposed to a complex mixture. Tables 2.21 through 2.23 present lists of organic contaminants in the environment and their LD_{50}.

2.7 Biological Weapons

Biological agents are organisms or toxins used to harm, kill, or incapacitate people. The three basic groups of biological agents that would likely be used as weapons by terrorists, criminals, or disgruntled individuals are bacteria, viruses, and toxins. Most biological agents are difficult to grow and maintain. They mostly break down quickly when exposed to sunlight and other environmental factors. Biological agents can be dispersed by spraying them into the atmosphere, by infecting livestock, and by contaminating food and water. Biological threats in different categories are provided in Tables 2.24 through 2.26.

2.8 Radiological and Nuclear Threats

Potential radiological threats are of three kinds. A terrorist or extremist group may actually steal a nuclear weapon, they may steal radioactive materials from chemical and ammunition plants, or they may attack a nuclear plant. Security experts

Table 2.20 Inorganic Chemicals LD_{50}

Contaminant	*LD_{50}*
Antimony	Oral rat LD_{50} 4,480 mg/kg (antimony acetate) Oral LD_{50} 115 mg/kg (antimony potassium tartrate) Oral LD_{50} 20,000 mg/kg (antimony(III)oxide)
Asbestos	Although asbestos is a known human carcinogen by the inhalation route, available epidemiological studies do not support the hypothesis that an increased cancer risk is associated with the ingestion of asbestos in drinking water
Barium	Oral rat LD_{50}: 355 mg/kg (barium nitrate) Oral rat LD_{50}: 118 mg/kg (barium chloride) The LD_{50} for rats: 630 mg/kg (barium carbonate) The LD_{50} for rats: 921 mg/kg (barium acetate)
Beryllium	Typical oral mouse LD_{50}: between 0.5 and 5 mg/kg
Cadmium	Acute oral toxicity rat LD_{50}: 890 mg/kg
Chromium	Human 0.5–1 g, oral—lethal (potassium chromate) Rat LD_{50} 1,800 mg/kg, oral (chromium(III)chloride) LD_{50} 3,250 mg/kg, oral (chromium(III)nitrate)
Cyanide	See Section 2.6.2
Fluoride	Oral LD_{50}: 60 mg F/kg body weight to 172 mg F/kg (fluoride) Oral rat LD_{50}: 125 g/kg (sodium fluorosilicate), corresponding to 12.5 g for a 100 kg adult
Mercury	Oral rat LD_{50}: 170 mg/kg, (anhydrous) 182 mg/kg, (dehydrate) Oral rat LD_{50}: 1 mg/kg ((mercury II) chloride) Oral rat LD_{50}: 18 mg/kg (mercury oxide) Oral rat LD_{50}: 46 mg/kg (mercuric thiocyanate)
Nickel	Oral rat LD_{50}: >5 g/kg
Nitrate	Oral rat LD_{50}: 200 mg/kg
Nitrite	Oral rat LD_{50}: 300 mg/kg

Table 2.20 (continued) Inorganic Chemicals LD_{50}

Contaminant	*LD_{50}*
Selenium	Oral rat LD_{50}: acute: 6,700 mg/kg
Thallium	Oral rat LD_{50}: 0.002 mg/kg

Note: See ATSDR (2010), California EPA (2010), MSDS (2010), Oxford University (2010), USEPA (2010c), ATSDR (2010).

have tried to analyze various scenarios such as the sabotage of vulnerable areas where radiological materials are stored or used. These scenarios have led to new approaches to tightening up security and improving intrusion prevention technologies. Table 2.27 provides a list of radiological terms.

2.8.1 Radiological Dispersion Device

A radiological dispersion device is a bomb that combines conventional explosives, such as dynamite, with radioactive materials in the solid, liquid, or gaseous form (NYDOH 2013). It is intended to disperse radioactive material into a small, localized area around an explosion (NYDOH 2013). The highest-grade radioactive materials are present in nuclear power plants and nuclear weapons sites; however, increased security at these facilities would make theft of these materials extremely difficult (NYDOH 2013).

2.8.2 Improvised Nuclear Device

An improvised nuclear device is a device incorporating radioactive materials designed to result either in the dispersal of radioactive material or in the formation of nuclear yield (US DoD 1993). Such devices may be fabricated in a completely improvised manner or may result from the sabotage, seizure, theft, or loss of a US or foreign nuclear weapon (US DoD 1993).

2.8.3 Nuclear Reactor Accident

A nuclear reactor accident is an uncontrolled reactor criticality resulting in damage to the reactor core such as loss of coolant that results in significant release of fission products from the reactor (US DoD 1993).

2.8.4 Nuclear Weapon

A nuclear weapon refers to a complete assembly (i.e., implosion type, gun type, or thermonuclear type) in its intended ultimate configuration which, upon completion of the prescribed arming, fusing, and firing sequence, is capable of producing the intended nuclear reaction and energy release (Joint Chiefs of Staff 2008). It

Table 2.21 Organic Contaminants

Contaminant	*Description*
Acrylamide (CAS no. 79-06-1)	Acrylamide is used in wastewater treatment, papermaking, ore processing, and the manufacture of permanent press fabrics. It also occurs in many cooked starchy foods, such as potato chips, french fries, and bread that has been heated.
Alachlor (CAS no. 15972-60-8)	Alachlor is a herbicide that is used to control annual grasses and broadleaf weeds.
Atrazine (CAS no. 1912-24-9)	Atrazine is a widely used herbicide to mitigate broadleaf and grassy weeds in major crops.
Benzene (CAS no. 71-43-2)	Benzene is used as an additive in gasoline and is an important solvent and precursor in the production of drugs, plastics, synthetic rubber, and dyes. It is discharged from factories and is leached from gas storage tanks and landfills.
Benzo(a)pyrene (PAHs) (CAS no. 50-32-8)	PAHs are produced as by-products of fuel burning. PAHs are also found in foods (e.g., cereal, oils, and fats).
Carbofuran (CAS no. 1563-66-2)	Carbofuran is one of the most toxic carbamate pesticides. It is used to control insects in a variety of field crops including rice, potato, corn, soybean, and alfalfa.
Carbon tetrachloride (CAS no. 56-23-5)	Discharge from chemical plants and other industrial activities.
Chlordane (CAS no. 57-74-9)	Residue of banned termiticide.
Chlorobenzene (CAS no. 108-90-7)	Discharge from chemical and agricultural chemical factories.
2,4-D (CAS no. 94-75-7)	Runoff from herbicide used on row crops.
Dalapon (CAS no. 75-99-0)	Runoff from herbicide used on rights of way.
1,2-Dibromo-3-chloropropane (DBCP) (CAS no. 96-12-8)	Runoff/leaching from soil fumigant used on soybean, cotton, pineapple, and orchards.
o-Dichlorobenzene (CAS no. 95-50-1)	Discharge from industrial chemical factories.

Table 2.21 (continued) Organic Contaminants

Contaminant	*Description*
p-Dichlorobenzene (CAS no. 106-46-7)	Discharge from industrial chemical factories.
1,2-Dichloroethane (CAS no. 156-60-5)	Discharge from industrial chemical factories.
1,1-Dichloroethylene (CAS no. 75-35-4)	Discharge from industrial chemical factories.
cis-1,2-Dichloroethylene (CAS no. 156-59-2)	Discharge from industrial chemical factories.
trans-1,2-Dichloroethylene (CAS no. 156-60-5)	Discharge from industrial chemical factories.
Dichloromethane (CAS no. 75-09-2)	Discharge from drug and chemical factories.
1,2-Dichloropropane (CAS no. 78-87-5)	Discharge from industrial chemical factories.
Di(2-ethylhexyl) adipate (CAS no. 103-23-1)	Discharge from chemical factories.
Di(2-ethylhexyl) phthalate (CAS no. 117-81-7)	Discharge from rubber and chemical factories.
Dinoseb (CAS no. 88-85-7)	Runoff from herbicide used on soybeans and vegetables.
Dioxin (2,3,7,8-TCDD) (CAS no. 1746-01-6)	Emissions from waste incineration and other combustion; discharge from chemical factories.
Diquat (CAS no. 85-00-7)	Runoff from herbicide use.
Endothall (CAS no. 145-73-3)	Runoff from herbicide use.
Endrin (CAS no. 72-20-8)	Residue of banned insecticide.
Epichlorohydrin (CAS no. 106-89-8)	Discharge from industrial chemical factories; an impurity of some water treatment chemicals.
Ethylbenzene (CAS no. 100-41-4)	Discharge from petroleum refineries.

(*continued*)

Table 2.21 (continued) Organic Contaminants

Contaminant	*Description*
Ethylene dibromide (CAS no. 106-93-4)	Discharge from petroleum refineries.
Glyphosate (CAS no. 1071-83-6)	Runoff from herbicide use.
Heptachlor (CAS no. 76-44-8)	Residue of banned termiticide.
Heptachlor epoxide (CAS no. 1024-57-3)	Breakdown of heptachlor.
Hexachlorobenzene (CAS no. 118-74-1)	Discharge from metal refineries and agricultural chemical factories.
Hexachlorocyclopentadiene (CAS no. 77-47-4)	Discharge from chemical factories.
Lindane (CAS no. 58-89-9)	Runoff/leaching from insecticide used on cattle, lumber, and gardens.
Methoxychlor (CAS no. 72-43-5)	Runoff/leaching from insecticide used on fruits, vegetables, alfalfa, and livestock.
Oxamyl (Vydate) (CAS no. 23135-22-0)	Runoff/leaching from insecticide used on apples, potatoes, and tomatoes.
Polychlorinated biphenyls (PCBs) (CAS no. 1336-36-3)	Runoff from landfills; discharge of waste chemicals.
Pentachlorophenol (CAS no. 87-86-5)	Discharge from wood preserving factories.
Picloram (CAS no. 1918-02-1)	Herbicide runoff.
Simazine (CAS no. 122-34-9)	Herbicide runoff.
Styrene (CAS no. 100-42-5)	Discharge from rubber and plastic factories; leaching from landfills.
Tetrachloroethylene (CAS no. 127-18-4)	Discharge from factories and dry cleaners.
Toluene (CAS no. 108-88-3)	Discharge from petroleum factories.
Toxaphene (CAS no. 8001-35-2)	Runoff/leaching from insecticide used on cotton and cattle.
2,4,5-TP (Silvex) (CAS no. 93-72-1)	Residue of banned herbicide.

Table 2.21 (continued) Organic Contaminants

Contaminant	*Description*
1,2,4-Trichlorobenzene (CAS no. 95-63-6)	Discharge from textile finishing factories.
1,1,1-Trichloroethane (CAS no. 71-55-6)	Discharge from metal-degreasing sites and other factories.
1,1,2-Trichloroethane (CAS no. 79-00-5)	Discharge from industrial chemical factories.
Trichlorethene (TCE) (CAS no. 79-01-6)	Discharge from metal-degreasing sites and other factories.
Vinyl chloride (CAS no. 75-01-4)	Leaching from PVC pipes; discharge from plastic factories.
Xylenes (total) (CAS no. 1330-20-7.)	Discharge from petroleum factories; discharge from chemical factories.

Source: US Environmental Protection Agency, Organic chemicals, http://water.epa.gov/drink/contaminants/#Organic, accessed January 2010, 2010b.

produces a nuclear detonation involving the joining (fusion) or splitting (fission) of atoms to produce an intense pulse or wave of heat, light, air pressure, and radiation (USDHHS 2005). The extent of damage depends on the power of the bomb and its destructive nature can be on the order of 100 times the bomb dropped on Hiroshima (USDHHS 2005). A nuclear detonation produces its damaging effects in four primary ways: blast, thermal radiation, ionizing radiation, and electromagnetic pulse (Joint Chiefs of Staff 2008). The radiation effects of a nuclear explosion are divided into two categories, initial and residual, as follows (Joint Chiefs of Staff 2008):

1. Initial radiation effects are those effects generated within the first minute following the detonation and are produced almost entirely from the nuclear processes occurring at detonation. These effects comprise the following:
   a. Initial radiation (e.g., gamma, neutron, x-ray) generated by the nuclear explosion and dependent upon the yield itself, which may be very harmful to humans and other life forms within a few miles of the explosion.
   b. Thermal radiation, which will ignite flammable materials and cause significant burns to people in the direct line of sight of the burst.
   c. Electromagnetic pulse, which may damage or destroy a variety of electronic equipment up to hundreds of miles away from the nuclear detonation.
2. Residual radiation is the radiation which is emitted later than 1 min after detonation. Its effects are caused by radioactive fallout and neutron-induced activity; it may encompass large areas, and serve as a persistent hazard to civilian and military personnel for extended periods of time.

Table 2.22 Volatile Organic Contaminants' Health Effects

Volatile Organic Chemicals	*Potential Health Effects*
Benzene	Cancer
Carbon tetrachloride	Liver effects, cancer
Chlorobenzene	Liver, kidney, nervous system effects
o-Dichlorobenzene	Liver, kidney, blood cell effects
p-Dichlorobenzene	Kidney effects, possible carcinogen
1,2-Dichloroethane	Cancer
1,1-Dichloroethylene	Liver, kidney effects, possible carcinogen
cis-1,2-Dichloroethylene	Liver, kidney, nervous system, circulatory system effects
trans-1,2-Dichloroethylene	Liver, kidney, nervous system, circulatory system effects
1,2-Dichloropropane	Cancer
Ethylbenzene	Liver, kidney, nervous system effects
Methylene chloride	Cancer
Styrene	Liver, nervous system effects, possible carcinogen
Tetrachloroethylene (PCE)	Cancer
Toluene	Liver, kidney, nervous system, circulatory system effects
Total THMs Chloroform Bromoform Bromodichloromethane Chlorodibromomethane	Cancer
1,2,4-Trichlorobenzene	Liver, kidney effects
1,1,1-Trichloroethane	Liver, nervous system effects
1,1,2-Trichloroethane	Kidney, liver effects, possible carcinogen
Trichlorethene (TCE)	Cancer

Table 2.22 (continued) Volatile Organic Contaminants' Health Effects

Volatile Organic Chemicals	*Potential Health Effects*
Vinyl chloride	Nervous system, liver effects, cancer
Xylenes (total)	Liver, kidney, nervous system effects
Bromate	Cancer
Chlorate	Anemia, nervous system effects
Haloacetic acids (HAA5)	Cancer
Total TTHMs	Cancer
Acrylamide	Cancer, nervous system effects
Alachlor	Cancer
Aldicarb	Nervous system effects
Aldicarb sulfoxide	Nervous system effects
Aldicarb sulfone	Nervous system effects
Atrazine	Liver, kidney, lung, cardiovascular effects; possible carcinogen
Benzo(a)pyrene (PAHs)	Liver, kidney effects, possible carcinogen
Carbofuran	Nervous system, reproductive system effects
Chlordane	Cancer
2,4-D	Liver, kidney effects
Di(2-ethylhexyl) adipate	Reproductive effects
Di(2-ethylhexyl) phthalate	Cancer
Dibromochloropropane (DBCP)	Cancer
Dinoseb	Thyroid, reproductive effects
Diquat	Ocular, liver, kidney effects
Endothall	Liver, kidney, gastrointestinal effects
Endrin	Liver, kidney effects
Epichlorohydrin	Cancer

(*continued*)

Table 2.22 (continued) Volatile Organic Contaminants' Health Effects

Volatile Organic Chemicals	*Potential Health Effects*
Ethylene dibromide (EDB)	Cancer
Glyphosate	Liver, kidney effects
Heptachlor	Cancer
Heptachlor epoxide	Cancer
Hexachlorobenzene	Cancer
Hexachlorocyclopentadiene (HEX)	Kidney, stomach effects
Lindane	Liver, kidney, nervous system, immune system, circulatory system effects
Methoxychlor	Developmental, liver, kidney, nervous system effects
Oxamyl (Vydate)	Kidney effects
Pentachlorophenol	Cancer
Picloram	Kidney, liver effects
Polychlorinated biphenyls (PCBs)	Cancer
Simazine	Body weight and blood effects, possible carcinogen
2,3,7,8-TCDD (Dioxin)	Cancer
Toxaphene	Cancer
2,4,5-TP (Silvex)	Liver, kidney effects

Note: See ATSDR (2010), California EPA (2010), MSDS (2010), Oxford University (2010), USEPA (2010).

2.9 Natural Disaster and Hazard

There are 14 types of natural disasters and hazards and weather emergencies that can negatively impact public safety, environment, critical infrastructures, and national safety as presented in Sections 2.9.1 through 2.9.14. Most of the natural hazards are considered in the engineering structural analyses and constructions of infrastructures, except *space weather*. In the United States, when building infrastructures near or adjacent to a floodplain or shoreline, engineers are required to delineate and specify the

Table 2.23 Organic Chemicals LD_{50}

Contaminant	*LD_{50}*
Acrylamide	Oral rat LD_{50}: 124 mg/kg Skin rat LD_{50}: 400 mg/kg
Alachlor	Oral rat LD_{50}: 930 and 1,350 mg/kg
Atrazine	Oral rat LD_{50}: 672–3,000 mg/kg Oral mouse LD_{50}: 850–1,750 mg/kg
Benzene	Oral rat LD_{50}: 930 mg/kg
Benzo(a)pyrene (PAHs)	Oral rat LD_{50}: 50 mg/kg
Carbofuran	Dermal rabbit LD_{50}: 6,783 mg/kg Oral rat LD_{50}: 7.34 mg/kg Inhalation rat LD_{50}: 0.10 mg/L/1 h
Carbon tetrachloride	Oral human LD_{LO}: 429 mg/kg Oral rat LD_{50}: 2,350 mg/kg Skin rabbit LD_{50}: >20,000 mg/kg
Chlordane	Oral rat LD_{50}: 200–700 mg/kg Oral mouse LD_{50}: 145–430 mg/kg
Chlorobenzene	Oral rat LD_{50}: 1,110 mg/kg Oral mouse LD_{50}: 2,300 mg/kg
2,4-D	Oral rat LD_{50}: 375–666 mg/kg Oral mouse LD_{50}: 370 mg/kg
Dalapon	Oral rat LD_{50}: 9,330–7,570 mg/kg
1,2-Dibromo-3-chloropropane (DBCP)	Oral rat LD_{50}: 170 mg/kg
o-Dichlorobenzene	Oral rat LD_{50}: 1,110 mg/kg
p-Dichlorobenzene	Oral rat LD_{50}: 500 mg/kg
1,2-Dichloroethane	Oral rat LD_{50}: 670 mg/kg Skin rabbit LD_{50}: 2,800 mg/kg Oral human LD_{LO}: 286 mg/kg
1,1-Dichloroethylene	Oral rat LD_{50}: 200 mg/kg

(*continued*)

Table 2.23 (continued) Organic Chemicals LD_{50}

Contaminant	*LD_{50}*
cis-1,2-Dichloroethylene	Oral rat LD_{50}: 770 mg/kg
trans-1,2-Dichloroethylene	Oral rat LD_{50}: 1,235 mg/kg
Dichloromethane	Oral rat LD_{50}: 1,600 mg/kg Oral human LD_{50}: 357 mg/kg
1,2-Dichloropropane	Oral rat LD_{50}: 1,947 mg/kg
Di(2-ethylhexyl) adipate	Oral rat LD_{50}: 9,100 mg/kg
Di(2-ethylhexyl) phthalate	Oral rat LD_{50}: 30 mg/kg
Dinoseb	Oral rat LD_{50}: 25–46 mg/kg
Dioxin (2,3,7,8-TCDD)	Oral rat LD_{50}: 0.022–0.045 mg/kg Oral hamster LD_{50}: 1 mg/kg
Diquat	Oral rat (female) LD_{50}: 231 mg/kg
Endothall	Oral rat LD_{50}: single dose of 40–60 mg/kg Oral dog LD_{50}: 20 or 50 mg/kg/day dose died within 3–11 days
Endrin	Oral rat LD_{50}: 7–43 mg/kg Oral rabbit LD_{50}: 60 mg/kg
Epichlorohydrin	Oral rat LD_{50}: 90 mg/kg
Ethylbenzene	Oral rat LD_{50}: 3,500 mg/kg
Ethylene dibromide	Oral rat LD_{50}: 108 mg/kg Oral mouse LD_{50}: 250 mg/kg Oral rabbit LD_{50}: 55 mg/kg
Glyphosate	Oral rat LD_{50}: 5,600 mg/kg
Heptachlor	Oral rat LD_{50}: 40–220 mg/kg Oral mouse LD_{50}: 30–68 mg/kg
Heptachlor epoxide	Oral rat LD_{50}: 15 mg/kg Oral rabbit LD_{50}: 144 mg/kg
Hexachlorobenzene	Oral rat LD_{50}: 10,000 mg/kg Oral guinea pig LD_{50}: 3,000 mg/kg

Table 2.23 (continued) Organic Chemicals LD_{50}

Contaminant	*LD_{50}*
Hexachlorocyclopentadiene	Oral mouse LD_{50}: 505 mg/kg Oral rat LD_{50}: 200 mg/kg
Lindane	Oral human LD_{100}: 150 mg/kg 10–20 mg/kg (acute toxicity) Oral rat LD_{50}: 88–190 mg/kg
Methoxychlor	Oral rat LD_{50}: 5,000–6,000 mg/kg Oral mouse LD_{50}: 1,850 mg/kg
Oxamyl (Vydate)	Oral rabbit LD_{50}: 2,960 mg/kg
Polychlorinated biphenyls (PCBs)	Oral rat LD_{50}: 1,900 mg/kg
Pentachlorophenol	Oral rat LD_{50}: 27–211 mg/kg Oral mouse LD_{50}: 74–130 mg/kg Oral rabbit LD_{50}: 70–300 mg/kg
Picloram	Oral rat LD_{50}: 8,200 mg/kg Oral mouse LD_{50}: 1,061–4,000 mg/kg Oral rabbit LD_{50}: 2,000–3,500 mg/kg
Simazine	Oral mouse LD_{50}: >5,000 mg/kg Dermal rabbit LD_{50}: 3,100–10,000 mg/kg
Styrene	Oral rat LD_{50}: 2,650 mg/kg Oral mouse LD_{50}: 316 mg/kg
Tetrachloroethylene	Oral rat LD_{50}: 2,629 mg/kg
Toluene	Oral rat LD_{50}: 636 mg/kg Dermal rabbit LD_{50}: 14,100 mg/kg Mouse vapor LC_{50}: 440 ppm for 24 h
Toxaphene	Oral hamster LD_{50}: 112–200 mg/kg Dermal LD_{50} for different species was determined as 300–1,000 mg/kg
2,4,5-TP (Silvex)	Oral mouse LD_{50}: 24 gm/kg

(*continued*)

Table 2.23 (continued) Organic Chemicals LD_{50}

Contaminant	*LD_{50}*
1,2,4-Trichlorobenzene	Oral rat LD_{50}: 756 mg/kg Dermal rat LD_{50}: 6,319 mg/kg
1,1,1-Trichloroethane	Oral rat LD_{50}: 9,600 mg/kg Oral rat LD_{50}: 6,000 mg/kg Dermal rabbit LD_{50}: 15,800 mg/kg Rat vapor LC_{50}: acute: 18,000 ppm for 4 h
1,1,2-Trichloroethane	Oral rat LD_{50}: <2,500 mg/kg Dermal rat LD_{50}: <4,300 mg/kg
TCE	Oral rat LD_{50}: 5,650 mg/kg Oral mouse LD_{50}: 2,402 mg/kg
Vinyl chloride	Oral rat LD_{50}: 500 mg/kg
Xylene	Oral rat LD_{50}: 4,300 mg/kg Inhalation rat LD_{50}: acute: 4,550 ppm for 4 h

Note: See ATSDR (2010), California EPA (2010), MSDS (2010), Oxford University (2010), USEPA (2010), ATSDR (2010).

engineering feasibility analysis of the risk of hazard and come up with recommendations not to build or to provide designs to mitigate risk that can impact the structural integrity of the infrastructures to protect public safety and would require insurance to cover any future damages. Accordingly, engineers should begin to consider explosive impacts on infrastructures to include protective measures when designing major infrastructures, once the vulnerability of the assets are measured. Federal and state governmental agencies should create requirements regarding these matters and then enforce engineers to include countermeasures in the engineering feasibility report, design, and construction.

2.9.1 Earthquakes

Earthquakes (seismic), also called temblors, can be tremendously destructive, and usually occur in the form of small tremors (NG 2013a). Earthquakes are the result of sudden movements of the Earth, caused by the release of strain that has accumulated over a long time. If the earthquake occurs in a populated area, it may cause deaths, injuries, and extensive property damage (NOAA 2013a). The Earth is formed of several layers that have different physical and chemical

Table 2.24 Biological Threats Category A

Category A indicates high-priority agents, which include organisms that pose a risk to national security	
Biological Agent	*Characteristic, Hazard, and Reduction Approach*
Anthrax (*Bacillus anthracis*)	Humans can contract spores from inhalation of aerosolized anthrax released during a biological weapon attack. Conditions ideal for propagation of anthrax include soil of pH > 6.0 rich in organic matter. LD_{50} for inhalational anthrax in humans from weapon-grade anthrax is 2,500–55,000 spores.
Botulism (*Clostridium botulinum* toxin)	Botulism is mainly a food-borne intoxication, but it can also be transmitted through wound infections or intestinal infection in infants.
Plague (*Yersinia pestis*)	*Yersinia pestis* is a serious issue because it contributes to waterborne and food-borne diseases such that each year it affects an estimated 76 million people in the United States. It can survive in water for 16 days and in moist soil for >60 days. It is inactivated by 1% sodium hypochlorite, but no reference to its tolerance to hypochlorite under usual conditions of drinking water disinfection has been recovered.
Smallpox (*variola major*)	After an incubation period of approximately 12 days, signs and symptoms include chills, fever, prostration, headache, backache, and vomiting, as well as pustule formation, with a case fatality rate among the unvaccinated of 25% or more (Eitzen et al. 1998). It is inactivated by 1% sodium hypochlorite, but no reference to its tolerance to hypochlorite under usual conditions of drinking water disinfection has been recovered.
Tularemia (*Francisella tularensis*)	Tularemia is an epizootic disease of animals (especially rabbits and rodents), transmissible to humans, caused by the bacillus *Francisella tularensis* (formerly *Pasteurella tularensis*). *F. tularensis* has been weaponized in the aerosol form. *P. tularensis* (*F. tularensis*) is 99.6%–100% inactivated by 0.5–1.0 mg/L fluorouracil adriamycin cyclophosphamide (FAC) at 10°C and pH 7 in approximately 5 min (Zilinskas 1997).

(*continued*)

Table 2.24 (continued) Biological Threats Category A

Category A indicates high-priority agents, which include organisms that pose a risk to national security	
Biological Agent	*Characteristic, Hazard, and Reduction Approach*
Viral hemorrhagic fevers	Viral hemorrhagic fevers may have been weaponized for aerosol application, but no reference has been recovered suggesting a potable water threat. Lassa fever virus is rapidly inactivated at 56°C; the other viruses require 30 min exposure at that temperature.

properties (NOAA 2013a). The outer layer consists of several large, irregularly shaped plates that slide over, under, and past each other on top of the partly molten inner layer (NOAA 2013a). Sometimes the movement of the plates is gradual. If the plates are locked together, the energy accumulates until it grows and becomes strong enough for the plates to break free (NOAA 2013a). Ninety percent of all earthquakes are found at crustal plate boundaries such as the Pacific Plate (NOAA 2013a). Earthquakes can also occur within plates, such as the New Madrid earthquakes of 1811–1812 and the 1886 Charleston earthquake which occurred within the North American plate (NOAA 2013a). Scientists assign a magnitude rating to earthquakes based on the strength and duration of their seismic waves. A quake measuring 3–5 is considered minor or light; 5–7 is moderate to strong; 7–8 is major; and 8 or more is great (NG 2013a). On average, a magnitude 8 quake strikes somewhere every year and some 10,000 people die in earthquakes annually (NG 2013a). Collapsing buildings claim by far the majority of lives, but the destruction is often compounded by mud slides, fires, floods, or tsunamis. Smaller temblors that usually occur in the days following a large earthquake can complicate rescue efforts and cause further death and destruction (NG 2013a). Surviving an earthquake and reducing its health impact requires preparation, planning, and practice (CDC 2013a). Far in advance, you can gather emergency supplies, identify and reduce possible hazards in your home, and practice what to do during and after an earthquake (CDC 2013a). Learning what actions to take can help you and your family to remain safe and healthy in the event of an earthquake (CDC 2013a).

2.9.2 Extreme Heat

Extreme heat is the number one weather-related killer in the United States, resulting in hundreds of fatalities each year (NOAA 2013b). In fact, on average, excessive heat claims more lives each year than floods, lightning, tornadoes, and hurricanes combined (NOAA 2013b). In the disastrous heat wave of 1980, more than

Table 2.25 Biological Threats Category B

Category B indicates the second highest priority agents, which include organisms that are moderately easy to disseminate	
Biological Agent	*Characteristic, Hazard, and Reduction Approach*
Brucellosis (*Brucella* species)	Brucellosis may survive in soil for 7–69 days and in water for 20–72 days; it is inactivated by direct sunlight (Parker et al. 1996). It is inactivated by 1% sodium hypochlorite, but no reference to its tolerance to hypochlorite under usual conditions of drinking water disinfection.
Epsilon toxin of *Clostridium perfringens*	*Clostridium perfringen*s is presumed to be indefinitely stable in sewage. It is a spore former used as an indicator organism and is relatively insensitive to inactivation by chlorine.
Food safety threats (e.g., *Salmonella* species, *Escherichia coli*, *Shigella*)	*Salmonella* survival in environmental media is 29–58 days in soil, 9 days in seawater, 8 days in freshwater, and up to 5 months in ice (White 1992). *Salmonella* survival is about the same. Because of the introduction of chlorine treatment of municipal water, waterborne typhoid has virtually disappeared in the United States.
Glanders (*Burkholderia mallei*)	Glanders may have been weaponized in aerosol form; a single reference suggesting its potential as an agent of drinking water contamination was recovered (Imangulov 1988). It survives in water at room temperature for up to 30 days in soil and for more than 27 days in water, but it is apparently not naturally found in soil or water. It is inactivated by 1% sodium hypochlorite water (Parker et al. 1996), but no reference to its tolerance to hypochlorite under usual conditions of drinking water disinfection was recovered.
Melioidosis (*Burkholderia pseudomallei*)	The most serious form of melioidosis in humans, an acute septicemic condition with diarrhea, has a high case-fatality rate if untreated. Parker et al. stated that it survives for years in soil and water. Melioisis is inactivated by 1% sodium hypochlorite (Parker et al. 1996), but no reference to its tolerance to hypochlorite under usual conditions of drinking water disinfection has been recovered.

(*continued*)

Table 2.25 (continued) Biological Threats Category B

Category B indicates the second highest priority agents, which include organisms that are moderately easy to disseminate	
Biological Agent	*Characteristic, Hazard, and Reduction Approach*
Psittacosis (*Chlamydia psittaci*)	Signs and symptoms of psittacosis include chills and fever, headache, sore throat, nausea, and vomiting; the case-fatality rate is ≤10% (31). It is considered susceptible to heat, similar to *Rickettsia prowazekii*. It is inactivated by 1% sodium hypochlorite (Parker et al. 1996), but no reference to its tolerance to hypochlorite under usual conditions of drinking water disinfection has been recovered.
Q fever (*Coxiella burnetii*)	Fever, cough, and pleuritic chest pain may occur as early as 10 days after exposure from Q fever. It survives in tap water for 160 days at 20°C–22°C and resists heat, drying, osmotic shock, and UV radiation. Hence, Q fever was reduced to undetectable levels in water treated with the ERDLator, a now-discontinued item of army field equipment that combined ferric chloride and limestone coagulation with 0.8 mg/L residual chlorine disinfection, 20 min contact time, and diatomite filtration. Under the same conditions, but with a chlorine residual of 0.5 mg/L, inactivation of Q fever was incomplete (Lindsten and Schmitt 1975).
Ricintoxin from *Ricinus communis* (castor beans)	The oral LD_{50} for mice is 20 mg/kg (Franz 1997). A conservative NOAEL would be 2 µg/L for water consumption of 15 L/day. It is detoxified in 10 min at 80°C and in ~1 h at 50°C (pH 7.8); it is stable under ambient conditions (Warner 1990). Hence, ricin is >99.4% inactivated after 20 min treatment with FAC at 100 mg/L, but it is essentially unchanged at 10 mg/L (Wannemacher et al. 1993). Iodine has no measurable effect at 16 mg/L. Reverse osmosis can efficiently remove ricin up to 99.8% from product water, but coagulation/flocculation was not effective. Using charcoal treatment system may effectively remove ricin. Further, some individual or point-of-use water purifiers may provide protection.
Staphylococcal Enterotoxin B (SEB)	SEB is an incapacitating toxin, causing severe gastrointestinal pain, projectile vomiting, and diarrhea if ingested; and fever, chills, headache, muscle aches, shortness of breath, and nonproductive cough if inhaled.

Table 2.25 (continued) Biological Threats Category B

Category B indicates the second highest priority agents, which include organisms that are moderately easy to disseminate	
Biological Agent	*Characteristic, Hazard, and Reduction Approach*
	The disinfection efficacy of SEB is unknown. Water treatment systems using charcoal should remove SEB (McGeorge 1989); thus, some individual and point-of-use water purifiers may provide protection.
Typhus fever (*Rickettsia prowazekii*)	Signs and symptoms of typhus fever include high fever, chills, intense headache, back and muscle pains, and skin eruptions (Freeman 1979). An infective dose of fewer than 10 organisms has been estimated, corresponding to a drinking water concentration of <1 organism per liter for consumption of either 15 L/day or 5 L/day for 7 days, if in fact epidemic typhus is transmissible through water (Parker et al. 1996). Typhus fever is inactivated by 1% sodium hypochlorite (Parker et al. 1996), but no reference to its tolerance to hypochlorite under usual conditions of drinking water disinfection has been recovered.
Viral encephalitis	Encephalomyelitis is usually an arthropod-borne disease of animals to which humans may be susceptible. No reference suggesting its potential as an agent of drinking water contamination has been recovered. It is inactivated by 1% sodium hypochlorite (Parker et al. 1996), but no reference to its tolerance to hypochlorite under usual conditions of drinking water disinfection has been recovered.
Water safety threat (*Cryptosporidium parvum*)	The signs and symptoms of cryptosporidiosis are profuse watery diarrhea, nausea, and stomach cramps. However, it has been suggested as a potential agent for sabotaging potable water supplies because of its infectivity and ready availability (Burrows and Renner 1999). An RO water purification unit can remove 100% of *Cr. parvum* oocysts, which are 3–7 μm in size. Removal of oocysts by direct filtration will approach 3 $\log_{10}$ in well-operated municipal systems (Clancy and Fricker 1998) and may exceed 5 $\log_{10}$ for slow sand filtration (SAIC 1996), but chlorination of the product water provides no protection if filtration performance degrades.

(*continued*)

Table 2.25 (continued) Biological Threats Category B

Category B indicates the second highest priority agents, which include organisms that are moderately easy to disseminate	
Biological Agent	*Characteristic, Hazard, and Reduction Approach*
Brucellosis (*Brucella* species)	The causative agents of brucellosis are *Brucella melitensis* and *Brucella suis*; the latter has been weaponized for aerosol application. Because brucellosis is contracted by the consumption of contaminated milk, it is prudent to consider water as a potential route of infection (Imangulov 1988). According to Parker, *Br. melitensis* may survive in soil for 7–69 days and in water for 20–72 days; it is inactivated by direct sunlight. *Br. melitensis* is inactivated by 1% sodium hypochlorite (Parker et al. 1996), but we did not find any reference to its tolerance to hypochlorite under usual conditions of drinking water disinfection.
Clostridium perfringens	*Clostridium perfringens* is a common organism in secondary sewage effluent. The spores may have potential for weaponization in aerosol form. No reference suggesting its potential as an agent of drinking water contamination has been recovered. *C. perfringens*, a spore former used as an indicator organism, is relatively insensitive to inactivation by chlorine. It is reduced by <1 $\log_{10}$ under treatment with a chlorine residual of 1.2 mg/L for 15 min at 20°C and a pH of approximately 7 (Tyrrell et al. 1995).

1250 people died. In the heat wave of 1995, more than 700 deaths in the Chicago area were attributed to heat. In August 2003, a record heat wave in Europe claimed an estimated 50,000 lives (NOAA 2013b). NOAA's heat alert procedures are based mainly on Heat Index Values (NOAA 2013b). The Heat Index, sometimes referred to as the apparent temperature and given in degrees Fahrenheit, is a measure of how hot it really feels when relative humidity is factored with the actual air temperature (NOAA 2013b). Heat disorders generally have to do with a reduction or collapse of the body's ability to shed heat by circulatory changes and sweating or a chemical (salt) imbalance caused by too much sweating (NOAA 2013b). These self-help measures are not a substitute for medical care but may help you recognize and respond promptly to warning signs of trouble (CDC 2013b). Your best defense against heat-related illness is prevention. Staying cool and making simple changes in your fluid intake, activities, and clothing during hot weather can help you remain safe and healthy (CDC 2013b).

Table 2.26 Biological Threats Category C

Category C indicates the third highest priority agents, which include emerging pathogens that could be engineered for mass distribution	
Biological Agent	*Characteristic, Hazard, and Reduction Approach*
Nipavirus	According to Sawatsky et al. (2008), the henipaviruses are naturally harbored by Pteropid fruitbats (flying foxes) and are characterized by a large genome, a wide host range, and their recent emergence as zoonotic pathogens capable of causing illness and death in domestic animals and humans. It can be inactivated by chlorine.
Hantavirus	Symptoms begin 1–6 weeks after inhaling the virus and typically start with 3–5 days of *flu-like* illness including fever, sore muscles, headaches, nausea, vomiting, and fatigue. As the disease gets worse, it causes shortness of breath because of fluid-filled lungs. It can be inactivated by chlorine.

2.9.3 Floods

A flood occurs when water overflows or inundates land that is normally dry. This can happen in a multitude of ways (NG 2013b). The most common is when rivers or streams overflow their banks (NG 2013b). Excessive rain, a ruptured dam or levee, rapid ice melting in the mountains, or even an unfortunately placed beaver dam can overwhelm a river and send it spreading over the adjacent land, called a floodplain (NG 2013b). Flooding typically occurs when prolonged rain falls over several days, when intense rain falls over a short period of time, or when an ice or debris jam causes a river or stream to overflow onto the surrounding area (NOAA 2013c). Flooding can also result from the failure of a water control structure, such as a levee or dam (NOAA 2013c). The most common cause of flooding is water due to rain or snow melt that accumulates faster than soils can absorb it or rivers can carry it away (NOAA 2013c). In the United States, where flood mitigation and prediction is advanced, floods do about $6 billion worth of damage and kill about 140 people every year (NG 2013b). Three-fourths of all presidential disaster declarations are associated with flooding (NOAA 2013c). A 2007 report by the Organization for Economic Cooperation and Development found that coastal flooding alone results in some $3 trillion damage worldwide (NG 2013b). In China's Yellow River valley, where some of the world's worst floods have occurred, millions of people have perished in floods during the last century (NG 2013b). Coastal flooding occurs when a large storm or tsunami causes the sea to surge inland (NG 2013b). Electrical power and natural gas or propane tanks should be shut off to avoid fire, electrocution, or explosions (CDC 2013c).

Table 2.27 Radiological Terms

Terms	*Description*
Acute radiation syndrome	Consists of three levels of effects: hernatopoletic (blood cells, most sensitive); gastrointestinal (GI cells, very sensitive); and central nervous system (brain/muscle cells, insensitive). The initial signs and symptoms are nausea, vomiting, fatigue, and loss of appetite. Below about 200 REM, these symptoms may be the only indication of radiation exposure.
Alpha particle (α)	The alpha particle has a very short range in air, and a very low ability to penetrate other materials, but it has a strong ability to ionize materials. Alpha particles are unable to penetrate even the thin layer of dead cells of human skin and, consequently, are not an external radiation hazard. Alpha-emitting nuclides inside the body as a result of inhalation or ingestion are a considerable internal radiation hazard.
Beta particles (β)	High-energy electrons emitted from the nucleus of an atom during radioactive decay. They normally can be stopped by the skin or a very thin sheet of metal.
Cesium-137 (Cs-137)	A strong gamma-ray source that can contaminate property, entailing extensive cleanup. It is commonly used in industrial measurement gauges and for irradiation of material. Half-life is 30.2 years.
Cobalt-60 (Co-60)	A strong gamma-ray source extensively used as a radiotherapeutic for treating cancer, food and material irradiation, gamma radiography, and industrial measurement gauges. Half-life is 5.27 years.
Curie (Ci)	A unit of radioactive decay rate defined as 3.7×10^{10} disintegrations per second.
Decay	The process by which an unstable element is changed to another isotope or another element by the spontaneous emission of radiation from its nucleus. This process can be measured by using radiation detectors such as Geiger counters.
Decontamination	The process of making people, objects, or areas safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.
Dose	A general term for the amount of radiation absorbed during a period of time.

Table 2.27 (continued) Radiological Terms

Terms	*Description*
Dosimeter	A portable instrument for measuring and registering the total accumulated dose to ionizing radiation.
Gamma rays (γ)	High-energy photons emitted from the nucleus of atoms; similar to x-rays. They can penetrate deeply into body tissue and many materials. Cobalt-60 and Cesium-137 are both strong gamma emitters. Shielding against gamma radiation requires thick layers of dense materials, such as lead. Gamma rays are potentially lethal to humans.
Half-life	The amount of time needed for half of the atoms of a radioactive material to decay.
Highly enriched uranium (HEU)	Uranium that is enriched to above 20% uranium-235 (U-235). Weapon-grade HEU is enriched to above 90% in U-235.
Ionize	To split off one or more electrons from an atom, thus leaving it with a positive electric charge. The electrons usually attach to one of the atoms or molecules, giving them a negative charge.
Iridium-192	A gamma-ray emitting radioisotope used for gamma radiography. The half-life is 73–83 days.
Isotope	A specific element always has the same number of protons in the nucleus. That same element may, however, appear in forms that have different numbers of neutrons in the nucleus. These different forms are referred to as "isotopes" of the element. For example, deuterium (2H) and tritium (3H) are isotopes of ordinary hydrogen (H).
Lethal dose (50/30)	The dose of radiation expected to cause death within 30 days to 50% of those exposed without medical treatment. The generally accepted range from 400 to 500 REM received over a short period of time.
Nuclear reactor	A device in which a controlled, self-sustaining nuclear chain reaction can be maintained with the use of cooling to remove generated heat.
Plutonium-239 (Pu-239)	A metallic element used for nuclear weapons. The half-life is 24–110 years.

(*continued*)

Table 2.27 (continued) Radiological Terms

Terms	*Description*
Rad	A unit of absorbed dose of radiation defined as deposition of 100 ergs of energy per gram of tissue. It amounts, approximately, to one ionization per cubic micron.
Radiation	High-energy alpha or beta particles or gamma-rays that are emitted by an atom as the substance undergoes radioactive decay.
Radiation sickness	Symptoms resulting from excessive exposure to radiation of the body.
Radioactive waste	Disposable, radioactive materials resulting from nuclear operations. Wastes are generally classified into two categories: high-level and low-level.
Radiological dispersal device (RDD)	A device (weapon or equipment), other than a nuclear explosive device, designed to disseminate radioactive material in order to cause destruction, damage, or injury by means of the radiation produced by the decay of such material.
Radioluminescence	The luminescence produced by particles emitted during radioactive decay.
Roentgen equivalent man (REM)	A REM is a unit of absorbed dose that takes into account the relative effectiveness of radiation that harms human health.
Shielding	Materials (lead, concrete, and so on) used to block or attenuate radiation for protection of equipment, materials, or people.
Special nuclear material (SNM)	Plutonium and uranium enriched in the isotope uranium-233 or uranium 235.
Uranium 235 (U-235)	Naturally occurring uranium U-235 is found at 0.72% enrichment. U-235 is used as a reactor fuel or for weapons; however, weapons typically use U-235 enriched to 90%. The half-life is 7.04×10^8 years.
X-ray	An invisible, highly penetrating electromagnetic radiation of much shorter wavelength (higher frequency) than visible light. Very similar to gamma-rays.

Source: US Central Intelligence Agency, Terrorist CBRN: Materials and effects, https://www.cia.gov/library/reports/general-reports-1/cbr_handbook/cbrbook.htm#6, accessed October 18, 2010 and January 1, 2013, 1998.

2.9.4 Hurricanes

Hurricanes (cyclones, typhoons, and other tropical storms) are giant, spiraling tropical storms that can pack wind speeds of over 160 miles per hour (mph) (257 km/h) and unleash more than 2.4 trillion gallons (9 trillion liters) of rain a day (NG 2013c). These same tropical storms are known as cyclones in the northern Indian Ocean and Bay of Bengal, and as typhoons in the western Pacific Ocean (NG 2013c). Hurricanes begin as tropical disturbances in warm ocean waters with surface temperatures of at least 80°F (26.5°C). Tropical cyclone is a generic term for a low-pressure system that usually forms in the tropics (NOAA 2013d). The cyclone is composed of powerful thunderstorms, and in the northern hemisphere, creates a counterclockwise circulation of winds near the Earth's surface (NOAA 2013d). These low-pressure systems are fed by energy from the warm seas. If a storm achieves wind speeds of 38 mph (61 km/h), it is known as a tropical depression (NG 2013c). A tropical depression becomes a tropical storm, and is given a name, when its sustained wind speeds top 39 mph (63 km/h) (NG 2013c). In the North Atlantic Ocean, the Northeast Pacific Ocean east of the dateline, or the South Pacific Ocean east of 160E, tropical cyclones are also called hurricanes, tropical storms, and tropical depressions, depending upon their intensity (NOAA 2013d). When a storm's sustained wind speeds reach 74 mph (119 km/h), it becomes a hurricane and earns a category rating of 1–5 on the Saffir–Simpson scale (NG 2013c). Be prepared to turn off electrical power when there is standing water, fallen power lines, or before you evacuate (CDC 2013d). Turn off gas and water supplies before you evacuate. Secure structurally unstable building materials (CDC 2013d).

2.9.5 Landslides and Mudslides

Landslides occur when masses of rock, earth, or debris move down a slope (CDC 2013e). *Debris flows*, also known as *mudslides*, are a common type of fast-moving landslide that tend to flow in channels (CDC 2013e). Landslides are caused by disturbances in the natural stability of a slope. They can accompany heavy rains or follow droughts, earthquakes, or volcanic eruptions (CDC 2013e). Mudslides develop when water rapidly accumulates in the ground and results in a surge of water-saturated rock, earth, and debris (CDC 2013e). Areas where wildfires or human modification of the land have destroyed vegetation on slopes are particularly vulnerable to landslides during and after heavy rains (CDC 2013e). In the United States, landslides and debris flows result in 25–50 deaths each year (CDC 2013e). The health hazards associated with landslides and mudflows include (CDC 2013e) (a) rapidly moving water and debris that can lead to trauma; (b) broken electrical, water, gas, and sewage lines that can result in injury or illness; and (c) disrupted roadways and railways that can endanger motorists and disrupt transport and access to health care.

2.9.6 Tornadoes

A tornado is a violently rotating column of air extending from a thunderstorm to the ground (NOAA 2013e). Tornadoes cause an average of 70 fatalities and 1500 injuries in the United States each year (NOAA 2013e). The strongest tornadoes have rotating winds of more than 250 mph and can be 1 mile wide and stay on the ground over 50 miles (NOAA 2013e). The average forward speed is 30 mph but may vary from nearly stationary to 70 mph (NOAA 2013e). During a tornado, people face hazards from extremely high winds and risk being struck by flying and falling objects (CDC 2013f). After a tornado, the wreckage left behind poses additional injury risks (CDC 2013f). Although nothing can be done to prevent tornadoes, there are actions you can take for your health and safety (CDC 2013f).

2.9.7 Tsunamis

A tsunami is a series of ocean waves caused by any large, abrupt disturbance of the sea surface (NOAA 2013f). Earthquakes cause most tsunamis, but a tsunami can also be generated by landslides, volcanic activity, or rarely by meteor impact (NOAA 2013f). If the disturbance is close to the coastline, a local tsunami can cause death and destruction among coastal communities within minutes (NOAA 2013f). While the frequency of damaging tsunamis in the US coastal areas is low compared to many other natural hazards, the impacts can be extremely high (NOAA 2013f). Tsunamis cannot be prevented but the impact of a tsunami can be mitigated through community preparedness, timely warnings, and effective response (NOAA 2013f). The majority of deaths associated with tsunamis are related to *drownings*, but traumatic injuries are also a primary concern (CDC 2013g). Injuries such as broken limbs and head injuries are caused by the physical impact of people being washed away into debris such as houses, trees, and other stationary items (CDC 2013g). As the water recedes, the strong suction of debris being pulled into large populated areas can further cause injuries and undermine buildings and services (CDC 2013g). Natural disasters do not necessarily cause an increase in infectious disease outbreaks (CDC 2013g). However, contaminated water and food supplies as well as the lack of shelter and medical care may have a secondary effect of worsening illnesses that already exist in the affected region (CDC 2013g).

2.9.8 Volcanoes

Volcanoes produce thick magma and large amounts of gas build up under the surface, causing eruptions that can be explosive, expelling lava, rocks, and ash into the air (NG 2013d). Less gas and more viscous magma usually mean a less dramatic eruption, often causing streams of lava to ooze from the vent (NG 2013d). Sixty percent of all active volcanoes are found at crustal plate boundaries such as the Pacific Plate (NOAA 2013g). Earth's crust, like the cracked shell of a hard-boiled

egg, is broken into a number of *plates* (NOAA 2013g). Where the plates are moving apart or colliding with one another, volcanoes may form and it can also form oceanic islands in the Pacific Ocean or Mediterranean Sea where *hot spots* occur in the crust and mantle (NOAA 2013g). These floating pieces of crust move about very slowly on the hotter interior (NOAA 2013g). A large eruption can be extremely dangerous for people living near a volcano (NG 2013d). Flows of searing lava, which can reach 2000°F (1250°C) or more, can be released, burning everything in its path, including whole towns (NG 2013d). Volcanoes can produce ash, toxic gases, flashfloods of hot water and debris called lahars, lava flows, and fast-moving flows of hot gases and debris called pyroclastic flows (CDC 2013h). Some of these threats can be predicted ahead of time and others may occur with little or no notice after an eruption occurs (CDC 2013h). About 1900 volcanoes on Earth are considered active, meaning they show some level of activity and are likely to explode again (NG 2013d).

2.9.9 Wildfires

On average, more than 100,000 wildfires, also called wildland fires or forest fires, clear 4–5 million acres (1.6–2 million hectares) of land in the United States every year (NG 2013e). In recent years, wildfires have burned up to 9 million acres (3.6 million hectares) of land (NG 2013e). A wildfire moves at a speed of up to 14 mph (23 km/h), consuming everything—trees, brush, homes, even humans—in its path (NG 2013e). There are three conditions that need to be present in order for a wildfire to burns which firefighters refer to as the fire triangle: fuel, oxygen, and a heat source (NG 2013e). The greater an area's fuel load, the more intensely the fire and air supply the oxygen that a fire needs to burn (NG 2013e). Lightning, burning campfires or cigarettes, hot winds, and even the sun can all provide sufficient heat to spark a wildfire. Smoke from wildfires is a mixture of gases and fine particles from burning trees and other plant materials (CDC 2013i). Smoke can hurt your eyes, irritate your respiratory system, and worsen chronic heart and lung diseases (CDC 2013i). The catastrophic fires of 1910 were a turning point in how the nation dealt with wildland fires (NOAA 2013h). Prior to 1910, there was no real concerted effort to manage or control the nation's forests or to fight forest fires (NOAA 2013h). The death and devastation left behind by the wildfires of 1910 brought it to the notice of the people, and as a result the US Forest Service (USFS) was tasked with managing the nation's forests and fighting wildfires (NOAA 2013h). In 1965, the USFS and the Bureau of Land Management (BLM) developed the Boise Interagency Fire Center (BIFC) to better coordinate firefighting efforts in the Great Basin area. Shortly after the development of the BIFC, the National Oceanic and Atmospheric Administration (NOAA) joined them (NOAA 2013h). In 1993, the BIFC changed its name to the National Interagency Fire Center (NIFC) (NOAA 2013h).

2.9.10 Winter Weather

Winter weather is extremely cold temperatures often accompanied by a winter storm, so you may have to cope with power failures and icy roads (CDC 2013j). Although staying indoors as much as possible can help reduce the risk of car crashes and falls on the ice, you may also face indoor hazards (CDC 2013j). Many homes will be too cold—either due to a power failure or because the heating system isn't adequate for the weather (CDC 2013j). Winter weather too often catches people unprepared (NOAA 2013i). Researchers say that 70% of the fatalities related to ice and snow occur in automobiles, and about 25% of all winter-related fatalities are of people who are caught off guard, out in the storm (NOAA 2013i). One of the gravest dangers of winter weather is wind chill. Wind chill is based on the rate of heat loss from exposed skin by the combined effects of wind and cold (NOAA 2013i). As the wind increases, heat is carried away from the body at an accelerated rate, decreasing the body temperature (NOAA 2013i). Animals are also affected by wind chill (NOAA 2013i). The National Snow and Ice Data Center (NSIDC) serves as the national information center that supports research in glaciers and freezing weather phenomena (NOAA 2013i).

2.9.11 Lightning

Cloud-to-ground lightning bolts are a common phenomenon—about 100 strike Earth's surface every single second—yet their power is extraordinary and each bolt can contain up to one billion volts of electricity (NG 2013f). A steplike series of negative charges, called a stepped leader, works its way incrementally downward from the bottom of a storm cloud toward the Earth. Each of these segments is about 150 ft (46 m) long. When the lowermost step comes within 150 ft (46 m) of a positively charged object, it is met by a climbing surge of positive electricity, called a streamer, which can rise up through a building, a tree, or even a person. The process forms a channel through which electricity is transferred as lightning (NG 2013f). About 2000 people are killed worldwide by lightning each year (NG 2013f).

2.9.12 Avalanches

Avalanches kill more than 150 people worldwide each year. Most are snowmobilers, skiers, and snowboarders (NG 2013g). Disastrous avalanches occur when massive slabs of snow break loose from a mountainside and shatter like broken glass as they race downhill, and these moving masses can reach speeds of 80 mph (130 km/h) within about 5 s (NG 2013g). Avalanches are most common during and in the 24 h right after a storm that dumps 12 in. (30 cm) or more of fresh snow (NG 2013g). Storminess, temperature, wind, slope steepness and orientation (the direction it faces), terrain, vegetation, and general snowpack conditions are all factors that influence whether and how a slope avalanches. Different combinations of these factors create low, moderate, considerable, and high avalanche hazards (NG 2013g).

2.9.13 Ultraviolet

Ultraviolet (UV) radiation is a silent hazard. The sun emits energy over a broad spectrum of wavelengths: visible light that you see, infrared radiation that you feel as heat, and UV radiation that you can't see or feel (NOAA 2013j). UV radiation has a shorter wavelength and higher energy than visible light (NOAA 2013j). It affects human health both positively and negatively (NOAA 2013j). Short exposure to UV radiation generates vitamin D, but can also lead to sunburn (NOAA 2013j).

2.9.14 Space Weather

Space weather describes the conditions in space that affect the Earth and its technological systems (NOAA 2013k). Space weather storms originate from the sun and occur in space near the Earth or in the Earth's atmosphere (NOAA 2013k). These storms generally occur due to eruptions on the sun known as solar flares and coronal mass ejections (CMEs) (NOAA 2013k). The sun's activity causes large changes in the sun's plasma and energetic particle populations, and these changes are responsible for the space weather that affects the Earth. Space weather can impact the upper atmosphere and may influence long-term climate trends (NASA 2012a). Technology is evolving at an incredible rate, especially our space-based technology. Many of these systems are vulnerable to hazardous space weather (NOAA 2013k). The health of this nation's technological infrastructure will depend heavily on our understanding of the space environment and our ability to predict hazardous solar storms (NOAA 2013k). With the rising sophistication of our technologies, and the number of people who use technology, vulnerability to space weather events has increased dramatically (NOAA 2013k). The aurora is a dynamic and visually delicate manifestation of solar-induced geomagnetic storms (NOAA 2013k). Geomagnetic storms (magnetic storms on the Earth due to solar activity) produce the *Aurora borealis* and *Aurora australis* (the Northern and Southern lights) but can also cause a variety of undesirable consequences (NASA 2012a). Geomagnetic storms induce electrical currents that can have significant impact on electrical transmission equipment (NOAA 2013k). Solar storms can also have significant impacts on the satellites we have come to rely on for everyday activities (NOAA 2013k). Electrical current surges in power lines, interference in the broadcast of radio, television, and telephone signals, and problems with defense communications are all associated with magnetic storms (NASA 2012b). These storms are known to alter the atmospheric ozone layer (NASA 2012b). Even increased pipeline corrosion has been attributed to them (NASA 2012b). High-energy solar protons can produce increased radiation in the atmosphere at altitudes where supersonic aircraft fly (NASA 2012a). This is especially true for flights over the north and south magnetic poles, areas unprotected by the Earth's magnetic field, where the radiation has direct access to the atmosphere (NASA 2012a). To reduce the risk to aircraft crews and passengers, and to reduce risk to the aircraft, routine forecasts

and alerts are sent through the Federal Aviation Administration so that a flight in potential danger can consider what course of action to take to minimize radiation exposure (NASA 2012a).

2.10 Cyberterrorism

A cyberattack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of September 11 (US DoD 2012). Clay Wilson (2005), in his report, identifies three different methods of attack, based on the effects of the weapons used:

- A *physical attack* involves conventional weapons directed against a computer facility or its transmission lines. A physical attack is implemented either through the use of conventional weapons, creating heat, blast, and fragmentation, or through direct manipulation of wiring or equipment, usually after gaining unauthorized physical access.
- An *electronic attack* (*EA*) involves the use of the power of electromagnetic energy as a weapon, more commonly as an electromagnetic pulse, to overload computer circuitry, but also in a less violent form, to insert a stream of malicious digital code directly into an enemy microwave radio transmission.
- A *computer network attack* (*CNA*) usually involves a malicious code used as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in computer security practices of an organization or computer user. Computer hackers opportunistically scan the Internet looking for computer systems that are misconfigured or lacking necessary security software.

By combining these concepts of intent and effects, *cyberterrorism* may be defined as the use of computers as weapons, or as targets, by politically motivated international or subnational groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies (Wilson 2005).

For military planners, the control of information is critical for success, and communications networks and computers are of vital operational importance (Wilson 2006). The use of technology to both control and disrupt the flow of information has been referred to by several names: information warfare, electronic warfare, cyberwar, netwar, and information operations (IO) (Wilson 2006). Wilson (2006) stated that an IO attack may take many forms, for example: (1) the software may be disrupted by transmitting a virus or other cyberweapons to slow adversary computers; (2) the computer circuitry may be overheated with directed high-energy pulse; and (3) powerful signals may be broadcast to create false images to misdirect enemy radar.

2.11 Implications

For pipeline, tunnel, and transportation engineers, it is very important nowadays to have awareness about terrorism hazards to incorporate security and defensive systems into engineering design considerations. Most engineers in this field of work and study are not fully acquainted with the lethality of man-made threats and how terrorists operate in academic and engineering professional organizations. The following chapter provides more discussions about disasters and acts of terrorism on pipelines, tunnels, underground rail, and transit systems. Chapter 3 also describes the following:

- Pipelines, tunnels, underground rail, and transit operations
- Clandestine subterranean infrastructures and tunnels
- Security for hazardous and radioactive material transshipments
- Impacts of vapor cloud explosion, flash fires, fireballs, pool fires, and jet flames
- Impacts of emission and dispersion of toxic substance
- Explosion destruction by missiles of fragments, objects, and sharp debris by burst
- Understanding of missile burst and flying glass

References

Agrawal, J. P. and Hodgson, R. D. 2007. *Organic Chemistry of Explosives*. West Sussex, UK: John Wiley & Sons.

Ahrens, H. 1977. *Propellants, Explos. Pyrotech*. 2(1–2):7–20.

Akhavan, J. 2004. *The Chemistry of Explosives*. Cambridge, UK: Royal Society of Chemistry.

Beck, W., Evers, J., Göbel, M., Oehlinger, G., and Klapötke, T. M. 2007. The crystal and molecular structure of mercury fulminate (Knallquecksilber). *Zeitschrift für anorganische und allgemeine Chemie* 663(9):1417–1422.

Boileau, J., Emeury, J. M., and Keren, J. P. 1975. German Patent 2,435,651 (February 6, 1975).

Burrows, W. D. and Renner, S. E. 1999. Biological warfare agents as threats to potable water. *Environ. Health Perspect*. 107(12):975–984.

California Environmental Protection Agency-Office of Environmental Health Hazard Assessment. 2010. Water Contaminants Information. http://www.oehha.org/water/phg/ (accessed January 23, 2011).

Centers for Disease Control and Prevention (CDC). 2013a. Earthquakes. http://www.bt.cdc.gov/disasters/earthquakes/ (accessed April 20, 2013).

Centers for Disease Control and Prevention (CDC). 2013b. Extreme heat. http://www.bt.cdc.gov/disasters/extremeheat/ (accessed April 20, 2013).

Centers for Disease Control and Prevention (CDC). 2013c. Floods. http://www.bt.cdc.gov/disasters/floods/after.asp (accessed April 20, 2013).

Centers for Disease Control and Prevention (CDC). 2013d. Hurricanes. http://www.bt.cdc.gov/disasters/hurricanes/readiness_factsheet.asp (accessed April 20, 2013).

Centers for Disease Control and Prevention (CDC). 2013e. Landsides and mudslides. http://www.bt.cdc.gov/disasters/landslides.asp (accesses April 20, 2013).

Centers for Disease Control and Prevention (CDC). 2013f. Tornadoes. http://www.bt.cdc.gov/disasters/tornadoes/ (accessed April 20, 2013).

Centers for Disease Control and Prevention (CDC). 2013g. Health effects of tsunami. http://www.bt.cdc.gov/disasters/tsunamis/healtheff.asp (accessed April 20, 2013).

Centers for Disease Control and Prevention (CDC). 2013h. Volcanoes. http://www.bt.cdc.gov/disasters/volcanoes/ (accessed April 20, 2013).

Centers for Disease Control and Prevention (CDC). 2013i. Wildfire. http://www.bt.cdc.gov/disasters/wildfires/facts.asp (accessed April 20, 2013).

Centers for Disease Control and Prevention (CDC). 2013j. About winter weather. http://www.bt.cdc.gov/disasters/winter/about.asp (accessed April 20, 2013).

Clancy, J. L. and Fricker, C. 1998. Control of cryptosporidium: How effective is drinking water treatment? *Water Qual. Int*. 4:37–41.

Dart, R. C. 2004. *Medical Toxicology*, pp. 1393–1401. Philadelphia, PA: Williams & Wilkins.

Doro-on, A. 2011. *Risk Assessment for Water Infrastructure Safety and Securty*. CRC Press Boca Raton, FL.

Eitzen, E., Pavlin, J., Cieslak, T., Christopher, G., and Culpepper, R. 1998. *Medical Management of Biological Casualties Handbook*, 3rd edn. Fort Detrick, MD: US Army Medical Research Institute of Infectious Diseases.

Emeury, J. L. and Girardon, H. H. 1980. Continuous process for the manufacture of Dinitroglycolurile (Dingu). US Patent 4,211, 874.

Franz, D. R. 1997. Defense against toxin weapons. In *Medical Aspects of Chemical and Biological Warfare*, eds. F. R. Sidell, E. T. Takafugi, and D. R. Franz, pp. 603–619. Washington, DC: TMM Publications.

Freeman, B. A. 1979. *Burrows Textbook of Microbiology*, 21st edn. Philadelphia, PA: WB Saunders.

Gibbs, T. R. and Poppolato, A. 1980. *LASL Explosive Property Data*. Berkeley, CA: University of California Press.

Hathaway, G. J., Proctor, N. H., Hughes, J. P., and Fischman, M. L. 1991. *Proctor and Hughes' Chemical Hazards of the Workplace*, 3rd edn. New York: Van Nostrand Reinhold.

Imangulov, R. J. 1988. *Medical Service and Protection from Weapons of Mass Destruction in the Subunits*, pp. 1–159. ICD 91-25. Aberdeen Proving Ground, MD: US Army Research Institute of Chemical Defense.

International Agency for Research on Cancer (IARC). 1987. *Overall Evaluations of Carcinogenicity: An Updating of IARC Monographs*, Vols. 1–42. IARC Monographs on the Evaluation of Carcinogenic Risks to Humans, supplement 7. Geneva, Switzerland: International Agency for Research on Cancer.

International Atomic Energy Agency (IAEA). 2003. WMD & global security: Time for reform. http://www.iaea.org/Publications/Magazines/Bulletin/Bull451/45103580406.pdf (accessed April 29, 2013).

International Cyanide Management Code for the Gold Mining Industry (ICMC). 2009. *Environmental and Health Effects of Cyanide*. Washington, DC: International Cyanide Management Code for the Gold Mining Industry.

International Programme on Chemical Safety (IPCS). 1996. Mustard gas. http://www.inchem.org/documents/pims/chemical/mustardg.htm (accessed May 2, 2013).

Jiang, Z. 2005. Shock waves. In *Proceedings of the 24th International Symposium on Shock Waves*, Beijing, China, July 11–14, 2004, Vol. 1, p. 984. Berlin, Germany: Springer.

Joint Chiefs of Staff. 2008. Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments, Joint Publication 3-11. http://www.dtic.mil/doctrine/new_pubs/jp3_11.pdf (accessed April 19, 2013).

Kingston, R. L., Hall, S., and Sioris, L. 1993. Clinical observations and medical outcome in 149 cases of arsenate and killer ingestion. *J. Toxicol. Clin. Toxicol*. 31(4):581–591.

Klaassen, C. and Watkins, J. 2003. *Casarett and Doull's Essentials of Toxicology*, p. 512. New York: McGraw Hill. ISBN 978-0071389143.

Knowles JR. 1980. Enzyme-catalyzed phosphoryl transfer reactions. *Annu. Rev. Biochem*. 49: 877–919.

Langefors, U. and Khilstrom, B. 1963. *The Modern Technique of Rock Blasting*. New York: Wiley.

Lawrence Berkeley National Laboratory (LBNL). 2010. Control procedures for chemicals with explosive properties. http://www.lbl.gov/ehs/chsp/html/cntrl-expl-chem.shtml (accessed April 29, 2013).

Ledgard, J. B. 2002. *Preparatory Manual of Explosives: A Comprehensive Laboratory Manual*. South Bend, IN: Paranoid Publications Group.

Lee, J. S. and Jaw, K. S. 2006. Thermal decomposition properties and compatibility of CL-20, NTO with silicon rubber. *J. Therm. Anal. Calorim*. 85:463–467.

Lee, J. S. and Jaw, K. S. 2008. Thermal decomposition properties and compatibility of CL-20, NTO with silicon rubber. *J. Therm. Anal. Calorim*. 93:953–957.

Lee, K. E., Hatch, R. L., Mezger, M., and Nicolich, S. 2001. High performance explosive containing CL-20. US Patent 6,214,137 B1 (April 10, 2001).

Lindsten, D. C. and Schmitt, R. P. 1975. Decontamination of water containing biological warfare agents. Report no. 2131, AD A014983. Fort Belvoir, VA: US Army Mobility Equipment Research and Development Center.

McGeorge, H. J. II. 1989. *Chemical/Biological Terrorism Threat Handbook*. Report DAALO3-86-D-0001. Aberdeen Proving Ground, MD: Chemical Research, Development and Engineering Center.

McNicol, L. J. P. 1966. Explosive lead azide process. US Patent 3,264,150. August 2, 1966.

Meyer, R., Kohler, J., and Homburg, A. 2002. *Explosives*, 5th edn. Weinheim, Germany: Wiley.

National Aeronautics and Space Administration (NASA). 2012a. Educational brief: Space weather. http://helios.gsfc.nasa.gov/ed-spcwthr.html (accessed April 20, 2013).

National Aeronautics and Space Administration (NASA). 2012b. Space weather. http://helios.gsfc.nasa.gov/weather.html (accessed April 20, 2013).

National Counterterrorism Center (NCTC). 2013. Common explosives. http://www.nctc.gov/site/technical/common_explosives.html (accessed April 29, 2013).

National Geographic (NG). 2013a. Earthquakes: Seismic destruction. http://environment.nationalgeographic.com/environment/natural-disasters/earthquake-profile/ (accessed April 20, 2013).

National Geographic (NG). 2013b. Floods. http://environment.nationalgeographic.com/environment/natural-disasters/floods-profile (accessed April 20, 2013).

National Geographic (NG). 2013c. Hurricanes. http://environment.nationalgeographic.com/environment/natural-disasters/hurricane-profile/ (accessed April 20, 2013).

National Geographic (NG). 2013d. Volcanoes. http://environment.nationalgeographic.com/environment/natural-disasters/volcano-profile/ (accessed April 20, 2013).

National Geographic (NG). 2013e. Wildfires: Dry, hot, and windy. http://environment.nationalgeographic.com/environment/natural-disasters/wildfires/ (accessed on April 20, 2013).

National Geographic (NG). 2013f. Lightning. http://environment.nationalgeographic.com/environment/natural-disasters/lightning-profile/ (accessed April 20, 2013).
National Geographic (NG). 2013g. Avalanches. http://environment.nationalgeographic.com/environment/natural-disasters/avalanche-profile/ (accessed April 20, 2013).
National Oceanic and Atmospheric Administration (NOAA). 2013a. Earthquakes. http://www.noaawatch.gov/themes/quake.php (accessed April 20, 2013).
National Oceanic and Atmospheric Administration (NOAA). 2013b. Excessive heat. http://www.noaawatch.gov/themes/heat.php (accessed April 20, 2013).
National Oceanic and Atmospheric Administration (NOAA). 2013c. Flooding. http://www.noaawatch.gov/themes/flooding.php (accessed April 20, 2013).
National Oceanic and Atmospheric Administration (NOAA). 2013d. Tropical weather. http://www.noaawatch.gov/themes/tropical.php (accessed April 20, 2013).
National Oceanic and Atmospheric Administration (NOAA). 2013e. Tornado. http://www.noaawatch.gov/themes/tsunami.php (accessed April 20, 2013).
National Oceanic and Atmospheric Administration (NOAA). 2013f. Tsunami. http://www.noaawatch.gov/themes/tsunami.php (accessed April 20, 2013).
National Oceanic and Atmospheric Administration (NOAA). 2013g. Volcanoes. http://www.noaawatch.gov/themes/volcanoes.php (accessed April 20, 2013).
National Oceanic and Atmospheric Administration (NOAA). 2013h. Fire weather. http://www.noaawatch.gov/themes/fire.php (accessed April 20, 2013).
National Oceanic and Atmospheric Administration (NOAA). 2013i. Winter weather. http://www.noaawatch.gov/themes/winter.php (accessed April 20, 2013).
National Oceanic and Atmospheric Administration (NOAA). 2013j. Ultraviolet (UV) radiation—A silent hazard. http://www.noaawatch.gov/themes/uv.php (accessed on April 20, 2013).
National Oceanic and Atmospheric Administration (NOAA). 2013k. Space weather. http://www.noaawatch.gov/themes/space.php (accessed April 20, 2013).
New York Department of Health (NYDOH). 2013. Dirty bomb. http://www.health.ny.gov/environmental/emergency/dirty_bombs.htm (accessed on April 19, 2013).
North Atlantic Treaty Organization. 2013. NATO's weapons of mass destruction initiatives. http://www.nato.int/cps/en/natolive/topics_50325.htm (accessed April 28, 2013).
Oregon Department of Human Service (ODHS). 2002. *Arsenic (As)*. Salem, OR: Office of Environmental Health, Environmental Toxicology Section, Oregon Department of Human Service.
Oxford University. 2010. Physical chemistry department standard material and data sheet. http://msds.chem.ox.ac.uk/HY/ (accessed August 2009 through October 2010).
Parker, A. C., Kirsi, J., Rose, W. H., and Parker, D. T. 1996. *Counter Proliferation—Biological Decontamination*. Report DAAD09-92-D-0004. Aberdeen Proving Ground, MD: US Army Test and Evaluation Command.
Parmeggiani, L. 1983. *Encyclopedia of Occupational Health and Safety*, 3rd revised edn. Geneva, Switzerland: International Labour Organisation.
Perry, D. L. and Phillips, S. L. 1995. *Handbook of Inorganic Compounds*. Boca Raton, FL: CRC Press.
Sawatsky, B., Ranaheera, C., Weingartl, H. M., and Czub, M. 2008. *Hendra and Nipah Virus. Animal Viruses: Molecular Biology*. Norwich, UK: Caister Academic Press.
Science Applications International Corp (SAIC). 1996. Ultraviolet light disinfection technology in drinking water application. An overview. EPA/811/R-96/002. Washington, DC: US Environmental Protection Agency.

Simpson, R. L., Urtiew, P. A., Ornellas, D. L., Moody, G. L., Scribner, K. J., and Hoffman, D. M. 1997. CL-20 performance exceeds that of HMX and its sensitivity is moderate. *Propellant, Explos. Pyrotech*. 22(5):249–255.

Standard Material Safety and Data Sheet (MSDS). 2010. Source of the chemicals or chemical compounds' MSDS. http://www.msdsonline.com (accessed 2008 through 2010).

Tyrrell, S. A., Rippey, S. R., and Watkins, W. D. 1995. Inactivation of bacterial and viral indicators in secondary sewage effluents, using chlorine and ozone. *Water Res*. 29(11):2483–2490.

United Nations (UN). 2012. NATO measures to prevent terrorists form acquiring weapons of mass destruction. http://www.un.org/disarmament/WMD/SGReport_Terrorism/Docs%202012/1st%20Cttee%20-%20IO%20replies%20-%202012/NATO%20-%20English.pdf (accessed April 28, 2013).

US Agency for Toxic Substances and Disease Registry (ATSDR). 2010. Toxic substances portal: Methyl tert-butyl ether (MTBE). http://www.atsdr.cdc.gov/toxfaqs/tf.asp?id=227&tid=41 (accessed July 29, 2010).

US Army and Air Force (USAAF). 1994. US Army Chemical Material Destruction Agency Old Chemical Weapons: Munitions Specification Report. http://www.lexpev.nl/downloads/oldchemicalweapons1994.pdf (accessed October 29, 2010).

US Central Intelligence Agency (CIA). 1998. Terrorist CBRN: Materials and effects. https://www.cia.gov/library/reports/general-reports-1/cbr_handbook/cbrbook.htm#6 (accessed October 18, 2010 and January 1, 2013).

US Central Intelligence Agency (CIA). 2010. Terrorist CBRN: Materials and effects. https://www.cia.gov/library/reports/general-reports-1/terrorist_cbrn/terrorist_CBRN.htm (accessed October 18, 2010 and January 1, 2013).

US Department of Defense (US DoD). 1993. DoD directive: Nuclear accident and incident public affair (PA) guidance, Number 5230.16. http://www.au.af.mil/au/awc/awcgate/dod/d523016p.pdf (accessed April 19, 2013).

US Department of Defense (US DoD). 1998. Integrating national guard and reserve component support for response to attacks using weapons of mass destruction. http://www.dod.mil/pubs/wmdresponse/ (accessed April 27, 2013).

US Department of Defense (US DoD). 2002. Environmental assessment for pulse fast neutron analysis cargo inspection test facility at Ysleta Port of Entry Commercial Cargo Facility, El Paso Texas. Dahlgren, VA: Counterdrug Technology Development Program Office, Naval Surface Warfare Center.

US Department of Defense (US DoD). 2007. Reducing vulnerabilities to weapons of mass destruction. http://www.acq.osd.mil/dsb/reports/ADA471566.pdf (accessed April 15, 2013).

US Department of Defense (US DoD). 2008. Chemical, Biological, Radiological and Nuclear Environments. http://www.dtic.mil/doctrine/new_pubs/jp3_11.pdf (accessed July 5, 2011).

US Department of Defense (US DoD). 2012. Panetta spells out DoD roles in cyberdefense. http://www.defense.gov/news/newsarticle.aspx?id=118187 (accessed on April 19, 2013).

US Department of Health and Human Services (USDHHS). 2005. Radiation emergencies. http://www.phe.gov/emergency/communication/guides/media/Documents/05.pdf (accessed April 19, 2013).

US Department of Homeland Security (US DHS). 2013. Ammonium nitrate security program. http://www.dhs.gov/ammonium-nitrate-security-program (accessed April 29, 2013).

US Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). 1984. Definition and test procedures of ammonium nitrate fertilizer. http://www.atf.gov/publications/download/hist/definition-and-test-procedures-for-ammonium-nitrate.pdf (accessed October 20, 2010).

US Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). 2010. Multiple searches on the characteristics of explosives. http://searchjustice.usdoj.gov/search?q=explosives+&site=default_collection&sort=date%3AD%3AL%3Ad1&output=xml_no_dtd&ie=UTF-8&oe=UTF-8&client=atf&proxystylesheet=atf (accessed July, 2010).

US Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). 2013. Ammonium nitrate security. http://www.atf.gov/explosives/programs/ammonium-nitrate-security/index.html (accessed April 29, 2013).

US Environmental Protection Agency (USEPA). 1987. Drinking water criteria document for cyanide. Prepared by the Office of Health and Environmental Assessment, Environmental Criteria and Assessment Office, Cincinnati, OH, for the Office of Drinking Water. Washington, DC: US Environmental Protection Agency.

US Environmental Protection Agency (USEPA). 2010a. Technical factsheet on cyanide. http://www.epa.gov/safewater/pdfs/factsheets/ioc/tech/cyanide.pdf (accessed January 5, 2010).

US Environmental Protection Agency (USEPA). 2010b. Organic chemicals. http://water.epa.gov/drink/contaminants/#Organic (accessed January 2010).

US Environmental Protection Agency (USEPA). 2010c. Inorganic chemicals. http://water.epa.gov/drink/contaminants/#Inorganic (accessed January 2010).

US Environmental Protection Agency (USEPA). 2010d. Ammonium nitrate. http://www.epa.gov/ttn/chief/ap42/ch08/final/c08s03.pdf (accessed October 4, 2010).

US Environmental Protection Agency (USEPA). 2010e. Explosives. http://www.epa.gov/ttn/chief/ap42/ch06/final/c06s03.pdf (accessed October 4, 2010).

US Environmental Protection Agency (USEPA). 2010f. Multiple searches on the characteristics of explosives. http://nlquery.epa.gov/epasearch/epasearch?querytext=Explosives&typeofsearch=epa&sort=term_relevancy&results_per_page=10&doctype=all&originalquerytext=Ammonium+Nitrate&areaname=&faq=no&filterclause=&sessionid=981E2B6116865D395E59B9D752558E2C&referer=http%3A%2F%2Fepa.gov%2F&prevtype=epa&result_template=epafiles_default.xsl&areasidebar=search_sidebar&areapagehead=epafiles_page head&areapagefoot=epafiles_pagefoot&stylesheet=http%3A%2F%2Fwww.epa.gov%2Fepafiles%2Fs%2Fepa.css&po=3333 (accessed May 2010).

US Government Accountability Office (US GAO). 2000. Weapons of mass destruction DoD's actions to combat weapons use should be more integrated and focused. GAO/NSIAD-00-97. http://www.gao.gov/assets/230/229156.pdf (accessed April 4, 2013).

US House of Representatives–Committee on Homeland Security (US HRCHS). 2013. Weapons of mass destruction. http://homeland.house.gov/issue/weapons-mass-destruction (accessed on April 24, 2013).

US Naval Technical Mission to Japan. 1945. Japanese bombs, intelligence targets Japan (DNI) of 4 September 1945, Fascicle 0-1, Target 0-23. http://www.fischertropsch.org/primary_documents/gvt_reports/USNAVY/USNTMJ%20Reports/USNTMJ_toc.htm (accessed October 26, 2010).

Verneker, V. R. and Forsyth, A. C. 1968. Mechanism for controlling the reactivity of lead azide. *J. Phys. Chem*. 72:111.

Wannemacher, R. W. Jr., Dinterman, R. E., Thompson, W. L., Schmidt, M. O., and Burrows, W. D. 1993. Treatment for removal of biotoxins from drinking water. Report no. TR9120, AD A275958. Fort Detrick, MD: US Army Biomedical Research and Development Laboratory.

White, G. C. 1992. *The Handbook of Chlorination and Alternative Disinfectants*, 3rd edn. New York: Van Nostrand Reinhold.

Wilson, C. 2005. Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress. CRC Report for Congress, Order Code RL32114. http://www.history.navy.mil/library/online/computerattack.htm (accessed April 20, 2013).

Wilson, C. 2006. Information operations and cyberwar: Capabilities and related policy issues. CRC Report for Congress, Order Code RL31787. http://www.hsdl.org/?view&did=441969 (accessed April 20, 2013).

Zilinskas, R. A. 1997. Iraq's biological weapons. The past as future? *JAMA* 278(5):418–424.

Chapter 3

Introduction to Pipelines, Tunnels, Underground Rail and Transit Operations, Terrorism, and Disasters

3.1 Introduction

This chapter provides fundamental engineering concepts of pipelines, tunnels, railways, underground freight transportation by capsule through pipelines, and other transit systems. Hazards and threats of terror attacks will be described in this chapter to identify some of the key areas and situations that should be considered for security and defense. There has been no ample data related to the magnitude of terrorism against pipelines, rails, and tunnels in the past and people tend to overlook the vulnerability of these infrastructures. Identifying some of the potential man-made disasters through this chapter can be a pathway to acknowledge small probabilities that could create grave consequences to national security based on the cumulative prospect theory and acceptable risk concepts so that people pay more attention and not disregard these probabilities as detailed in Chapters 6 and 7. Additionally, secret subterranean infrastructures and illegal production and transport of weapons of mass destruction (WMD) will be analyzed to determine what procedures are needed to control these unlawful acts as a support to homeland

security and defense. The main purpose of this chapter is to bridge the gap between engineering and homeland protection—to enable engineers visualize the magnitude of risk of terror attacks against infrastructures presented in this book, to incorporate security components in the future engineering design, and finally to allow homeland security professionals understand the engineering operations so that they can also provide stronger security foundations to reduce negative impacts of terrorism and disaster.

3.2 Disaster and Acts of Terrorism against Pipelines, Tunnels, and Underground Rail and Transit Systems

Pipelines, tunnels, and underground rail transports are some of the prime economic mechanisms not only in the United States but also in other nations; however, these infrastructures remain vulnerable to sabotage. Multiple disasters can be created by terrorists: for instance, intentional automobile accidents with two rail transits causing disruptions that will produce explosions of gas or petroleum pipelines. On June 4, 1989, two trains were involved in an accident that resulted in an explosion of a gas pipeline near Ufa, Russia, in which there were approximately 645 casualties and 800 injured. A similar event can easily occur in a single terror attack within a large metropolitan area in the United States, Russia, Middle East, Asia, and Europe when no advanced protective systems are applied. Paul Parfomak (2004) stated that, some 470,000 miles of oil and gas transmission pipelines crisscross the United States, with links to Mexico and Canada. There are 88,000 miles of crude pipelines, 254,000 miles of transmission pipelines, 91,000 miles of product lines, 981,000 miles of freight pipelines, 120,986 miles by Class 1 freight railroads, 21,250 miles by regional freight railroads, 28,422 miles by local freight railroads, and 22,741 miles by Amtrak passenger rails (DOT/BOT 2002).

According to Badkar (2012), Helman (2010), OPEC (2011), and BP Energy (2011, 2012), some of the current and future top oil producers in the world are Ghawar, Saudi Arabia (30 billion barrels; current and future); Khurais, Saudi Arabia (27 billion barrels in the future); the entire Saudi Arabia (265 billion barrels); Carabobo, Venezuela (15 billion barrels in the future); the entire Venezuela (211 billion barrels); Khuzestan, Iran (100 billion barrels in the future); the entire Iran (137 billion barrels); West Qurna, Iraq (21 billion barrels in the future); Majnoon, Iraq (13 billion barrels in the future); Rumaila, Iraq (17 billion barrels); the entire Iraq (115 billion barrels); Kuwait (102 billion barrels); United Arab Emirates (98 billion barrels); Khurais, Russian Federation (77 billion barrels); Libya (46 billion barrels); Kashagan, Kazakhstan (9 billion barrels in the future), the entire Kazakhstan (40 billion barrels); Nigeria (37 billion barrels); Canada (32 billion barrels); United States (31 billion barrels); Qatar (26 billion barrels); China (15 billion barrels), Tupi, Brazil (8 billion barrels in the future); the entire Brazil (14 billion barrels); North Slope, Alaska (up to 40 billion barrels in the future).

These figures show that these nations have substantial pipeline systems that need to be secured. Approximately more than 75% of the top oil producers' pipeline systems are located in the areas with higher risk of terrorism.

Automated underground freight transportation through pipeline, tubular rail, and underground magnetic levitation transport system (also known as *maglev train*) is considered to be a highly advanced transport technology and is becoming more favorable in northern Europe, Asia (China, Japan, and South Korea), Iran, and the United States. As these are different from other conventional rail systems such as newly adopted transportation technologies for goods and passengers, security against terrorism has not been entirely analyzed and the negative impacts of intentional man-made disaster are not fully defined. The following sections will provide detailed operations and structural components, including potential threats against these new rail systems.

3.2.1 Security for Hazardous and Radioactive Material Transport Systems

In the aftermath of the terrorist attacks on September 11, 2001, there was heightened concern about the probability for terrorists to highjack a truck carrying hazardous materials (HAZMAT) or use it in some other fashion to commit a terrorist act (DOT 2004a). The Federal Motor Carrier Safety Administration (FMCSA) made over 32,000 contacts and security-sensitive visits with HAZMAT carriers (DOT 2004a). These contacts and visits resulted in over 280 findings of "suspicious activity" and over 125 referrals to the Federal Bureau of Investigation (FBI) (DOT 2004a). The Transportation Security Administration (TSA) is gradually implementing Section 1012 of the USA PATRIOT Act (P.L. 107-56) (Rothberg 2005). This provision seeks to reduce some of the security risks associated with HAZMAT transportation by requiring a security threat assessment of drivers with a HAZMAT endorsement on their commercial driver license (CDL) (Rothberg 2005). HAZMAT shipments through intermodal connectors, modes, and facilities are all prospective targets for domestic acts of terrorism, and pose a much greater concern to public safety than most other shipment types (DOT 2003a). As much as 95% of HAZMAT shipments are transported via motor carriers and safeguards should be in place to help protect against the HAZMAT shipper, motor carrier, and recipient, plus the surrounding community that would experience a direct and immediate negative economic impact following an incident (DOT 2003a). In the United States, approximately 800,000 shipments of HAZMAT are transported each day in bulk and in smaller shipment configurations (DOT 2003b). With regard to bulk rail shipments, the industry uses rail tank cars (DOT 2003b). A subset of these cars moves over 275,000 shipments of chlorine, anhydrous ammonia, propane gas, and gasoline every year (DOT 2003b). The motor carrier industry dedicates more than 400,000 large trucks to the transportation of HAZMAT (DOT 2003b). A subset of this fleet participates

in approximately 18,800,000 shipments of gasoline and 125,000 shipments of explosives a year (DOT 2003b). HAZMAT is an especially sought-after target because the nature of the cargo severs as a dangerous and ready-made weapon (DOT 2004b). According to the Department of Transportation (DOT 2004b), the immediate damage from a terrorist attack could be severe in terms of both human and economic losses. Human losses could be both injuries and death, with up to 10,000 casualties (DOT 2004b).

According to the Department of Energy (DOE) (1999), radioactive material is any material that contains unstable (radioactive) atoms (DOE 1999). Radioactivity is the process of unstable (or radioactive) atoms trying to become stable (DOE 1999). This is done by emitting radiation in the form of alpha particles, beta particles, neutron particles, and gamma rays. Certain DOE shipments, including weapons and weapons parts, are classified to protect the shipments and national security (DOE 1999). The World Nuclear Association (WNA 2011) stated that about 20 million consignments of radioactive material (which may be either a single package or a number of packages sent from one location to another at the same time) take place around the world each year. Radioactive materials are used extensively in medicine, agriculture, research, manufacturing, nondestructive testing, and minerals' exploration (WNA 2011).

In the United States, 1% of the 300 million packages of hazardous material shipped each year contain radioactive materials (WNA 2011). About 3 million packages of radioactive materials are shipped each year in the United States (DOE 1999). International regulations for the transport of radioactive materials have been published by the International Atomic Energy Agency (IAEA) since 1961 (WNA 2011). According to the International Atomic Energy Agency (IAEA 2006), the United Nations (UN) approved the statutes of the IAEA in October 1956, and these statutes entered into force on July 29, 1957. While safety is a national responsibility, international standards and approaches to safety promote consistency, help to provide assurance that nuclear- and radiation-related technologies are used safely, and facilitate international technical cooperation and trade (IAEA 2005). The IAEA Regulations apply to the transport of radioactive material by all modes on land, water, or air, including transport which is incidental to the use of the radioactive material (IAEA 2005). However, these Regulations do not specify controls such as routing or physical protection which may be instituted for reasons other than radiological safety (IAEA 2005).

In operation since the 1960s, the safeguard system of the IAEA is a central component of the world's commitment to control the spread of nuclear weapons (IAEA 2006). Under the agreements that Member States conclude with the IAEA, inspectors regularly visit nuclear facilities to verify records that state authorities keep the whereabouts of nuclear material under their control, check IAEA-installed instruments and surveillance equipment, and confirm physical inventories of nuclear materials (IAEA 2006). These and other safeguard measures provide independent, international verification that governments are living up to their

commitments to peaceful uses of nuclear technology (IAEA 2006). In determining the security measures to be implemented for the radioactive material in transport, a number of topics need to be considered to prevent the unauthorized access to, or theft of, or other malicious acts involving, the material (IAEA 2008). The IAEA (2008) pointed out that the transport security system should be designed to take into account

1. The quantity and the physical and chemical form of the radioactive material.
2. The modes of transport.
3. The packages being used.
4. Measures that are required—to deter, detect, and delay unauthorized access to the radioactive material while in transport and during storage in transit to defeat any attempted malicious acts, to identify the actual possible malicious acts involving any consignment while in transport or during storage incidental to transport to enable an appropriate response and to allow recovery or mitigation efforts to start as soon as possible, to provide rapid response to any attempts directed toward, or actual, unauthorized access to radioactive material.
5. Capabilities for recovering any damaged, stolen, or lost radioactive material and bringing it under secure regulatory control and minimizing and mitigating the radiological consequences of any theft, sabotage, or other malicious act.

3.2.2 Fire, Explosion, and Detonation

The major hazards in oil and gas pipeline, tunnel, and rail systems are fire, explosion, and detonation. The consequences of these three major hazards not only results in casualties, and severe property and environmental damages, but also leave the public with a lower level of confidence. Fire is the rapid oxidation, usually with the evolution of heat and light, of a heat fuel, oxygen, and the interaction of the three (NWCG 2011). Flash fires and fireballs emit excessive heat that can be deadly. There are several classifications of fire based on the National Fire Protection Association (NFPA) Codes as follows (NWCG 2011, NFPA 2012b):

1. Class A, fires involving ordinary combustible materials requiring the heat-absorbing effects of water, water solutions, or the coating effects of certain dry chemicals, which retard combustion
2. Class B, fires involving flammable or combustible liquids, flammable gases, greases, and similar materials where extinguishment is most readily secured by excluding air (oxygen), inhibiting the release of combustible vapors, or interrupting the combustion chain reaction
3. Class C, fires involving live electrical equipment where safety to the operator requires the use of electrically nonconductive extinguishing agents

4. Class D, fires involving certain combustible metals (magnesium, titanium, zirconium, sodium, potassium, etc.) requiring a heat-absorbing extinguishing medium not reactive with burning metals
5. Class K, fires in cooking appliances that involve combustible cooking media

The NFPA 20113 (2012a) explained that flash fire may occur in an environment where fuel and air are mixed to combust with a heat flux approximately 84 kW/m^2. The majority of road tunnels of significant length have some form of ventilation system for various reasons including smoke control in a fire emergency (Carvel et al. 2009). These fall broadly into two categories—transverse systems and longitudinal systems—although an increasing number of tunnels, for example, the refurbished Mont Blanc tunnel (Brichet et al. 2002), have elements of both types installed (Carvel et al. 2009). Transverse ventilation systems use air ducts, generally either above a false ceiling within the tunnel or below the road deck, to supply and extract air at periodic locations along the length of the tunnel; extraction is only carried out at a small number of locations, and such systems are known as semi-transverse systems (Carvel et al. 2009). Longitudinal systems use jet fans, generally mounted on the ceiling, to move air along the main tunnel void (Carvel et al. 2009). In addition, water mist systems are unable to suppress or control large fires; therefore, the *design fire* for a water mist system in a tunnel should not be specified in terms of peak heat release rate, but rather in terms of the characteristics of a growing fire which such a system is designed to suppress (Carvel 2008).

Explosion is an abrupt increase in volume, rapid change in pressure, and release of energy with high temperatures and gases, which generates a shock wave. Detonation is caused by a reaction from explosive material that creates a shock wave. A ruptured oil and gas pipeline can cause a massive explosion and can lead to public and environmental injury. The US pipeline system is an extensive mode of transportation with unique infrastructure security characteristics and requirements (TSA 2012). Vast networks of pipelines crisscross thousands of miles to transport nearly all the natural gas and approximately 65% of hazardous liquids, including crude and refined petroleum products that are consumed in the United States (TSA 2012). There are approximately 3,000 companies in the United States that operate (TSA 2012): (a) 175,000 miles of hazardous liquid pipelines; (b) 321,000 miles of natural gas transmission pipelines; and (c) 2.06 million miles of natural gas distribution pipelines. Other countries such as Egypt are having a hard time with security in the Sinai Peninsula (UPI 2011a). Israel and Jordan meet a significant amount of their energy demands through Egyptian natural gas (UPI 2011a). For the ninth time since the Egyptian revolution, saboteurs have attacked the natural gas pipeline in the Sinai Peninsula (UPI 2011b). Israel gets about one-quarter of its electricity needs from natural gas supplied through Egypt, while Jordan imports most of the energy it needs (UPI 2011b). Al Qaeda in the Arabian Peninsula has also launched attacks on oil and natural gas pipelines in Yemen (UPI 2012a). Additionally, an attack on a natural gas pipeline in western Syria caused a loss of electricity in parts

of the country (UPI 2012b). Energy companies operating in Syria declared force majeure, meaning they could not carry out contractual obligations because of circumstances beyond their control (UPI 2012b).

3.2.2.1 Vapor Cloud Explosion and Jet Flames

Gas explosions can generate pressure known as vapor cloud explosion where the flame front moves through the unconfined gas cloud. If the flame is moving rapidly, the gas–air mixture is unable to transport from the flame adequately to allow free expansion of the combustion products generated by the flame. A vapor cloud explosion can be seen from a ruptured oil pipeline or rail carrying a flammable liquid in an accident. Jet flames are created from a partially confined volume into another gas cloud.

3.2.2.2 Flash Point

Flash point is the minimum temperature at which a liquid gives off vapor within a test vessel in sufficient concentration to form an ignitable mixture with air near the surface of the liquid (OSHA 1996, 2012). Flammable solvents have flash points below 37.8°C (100°F). Their vapor pressure rises with temperature and as temperatures increase they become more ignitable. Flammables have a minimum concentration below which propagation of flame does not occur upon contact with a source of ignition. This is known as the *lower flammable explosive limit* (LEL) (OSHA 1996, 2012). There is also a maximum concentration of vapor or gas in air above which propagation of flame does not occur (OSHA 1996, 2012). This is known as the *upper flammable explosive limit* (UEL) (OSHA 1996, 2012). These units are expressed in percentage of gas or vapor in air by volume (OSHA 1996, 2012).

3.2.2.3 Flammability Range

The *flammability range* (FR) of a flammable solvent defines the level of air and vapor mixtures that can ignite. It is characterized by the *upper flammability limit* (UFL) and *lower flammability limit* (LFL). The mixture is not ignitable when the level of air and vapor mixtures is not within the UFL and LFL.

3.2.2.4 Autoignition Temperature

The *autoignition temperature* is the temperature at which a substance will spontaneously combine with oxygen and burn without an external ignition or heat source (Yale University 2012). Solvents with low autoignition temperatures have been known to ignite when placed in contact with hot surfaces such as hot plates (Yale University 2012). For a fire to occur, three distinct conditions must exist simultaneously (Yale University 2012): (1) the concentration of the vapor must be between

the UFL and LFL of the substance (the right fuel/air mix); (2) an oxidizer, usually the oxygen in air, must be available; and (3) a source of ignition must be present. Removal of any of these three conditions will prevent the start of a fire.

3.2.2.5 Flame Speed and Burning Velocity

The flame speed is the calculated rate of expansion of the flame front in a combustion reaction. It is the same as explosive velocity but is applied for a fuel, to measure the rate of ignitability. The velocity at which the combustible gases move through a flame in the direction perpendicular to the flame surface defines the *burning velocity* (McGraw-Hill 2012).

3.2.2.6 Pool Fires

The expression heat released rate (HRR) versus time (t) describes fire development. Thus, delineating the HRR, also known as the burning rate Q, is critical in *fire hazard analysis* in infrastructure disaster and is usually determined by testing. The relationship between Q and t for a certain fire scenario is defined as the design fire curve for that scenario, as illustrated in Figure 3.1. For a routine *fire hazard analysis* in infrastructure protection, it is acceptable to approximate the burning rates. An example is that, post-burst infrastructure analyses are usually based on the fire severity associated with an aggregate fuel loading. Table 3.1 lists some HRR characteristic sources. The HRR can be calculated using the following equation: $\rho_0 D = \rho_1 (D - W) : v_1 D = v_0 (D - W)$. A horizontal upward-facing combustible fuel characterizes a pool fire. A pool fire signifies the fuel in

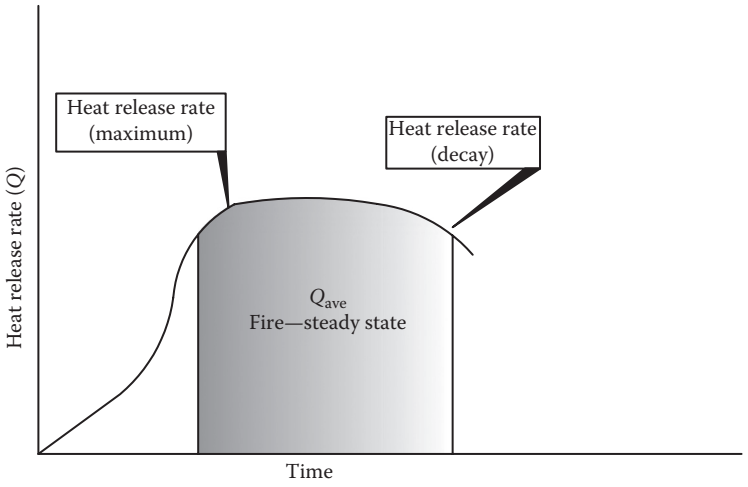


Figure 3.1 Design fire curve.

Table 3.1 Pipeline Failure, Disaster, and Terrorism

Year	*Event*	*Cause/Location*	*References*
1971	Over 80 transmission line failures occurred in pipelines due to shaking.	San Fernando earthquake (California)	Ballantyne (2008)
1989	PG&E had three failures of transmission lines, and extensive damage to the cast iron distribution system in the San Francisco Marina District resulting in an extensive cast iron pipe replacement program using polyethylene.	Loma Prieta earthquake (California)	Earthquake Engineering Research Institute (1990)
1994	There were 209 repairs required to metallic distribution lines and 27 to polyethylene lines.	Northridge earthquake (California)	Ballantyne (2008)
1997	Williams natural gas pipeline ruptured.	Landslide and ignition (Washington)	Whatcom County Planning (2001)
1999	Olympic petroleum product pipeline ruptured in Whatcom Falls Park, killing two children and a young man and causing extensive property and environmental damage when around 250,000 gal of gasoline spilled and ignited.	Ruptured pipeline (Washington)	Whatcom County Planning (2001)
2010	A 30 in. diameter segment of an intrastate natural gas transmission pipeline known as Line 132, owned and operated by the Pacific Gas and Electric Company, ruptured in a residential area in San Bruno, California. The rupture produced a crater of about 72 ft long × 26 ft wide. The released natural gas ignited, resulting in a fire that destroyed 38 homes and damaged 70. Eight people were killed, many were injured, and many more were evacuated from the area.	Accident, rupture pipe	National Transportation Safety Board (2011)

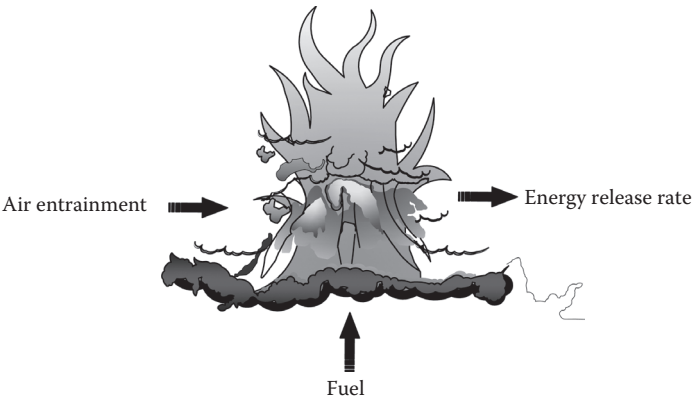


Figure 3.2 Dynamic feature of a pool fire.

liquid phase or any solid fuels that decompose similar to liquids. Typically, when liquid fuel is spilled, the flammable liquid may form a pool of any shape and thickness and can be controlled depending on the geometry of the confinement area. After an explosion, a pool fire spreads rapidly over the liquid spill and a flame spread rate starts at approximately 10 m/s. Figure 3.2 depicts the dynamic feature of a pool fire.

3.2.3 Emission and Dispersion

Fire explosion and toxic/hazardous release result in emission and dispersion of the chemical substance or material. There are two phases that generate the aforementioned conditions:

1. Release of flammable material and oxygen mixture in the atmosphere, and development of flammable cloud which turns into a fire and vapor cloud explosion
2. Release of hazardous material which contaminates the site and environment, possibly affecting public health in the surrounding area

There are several kinds of situations which can result in emission (e.g., HAZMAT freight transportation accidents or oil pipeline bursts). The emission of toxic material resulting from terrorist attacks has been the growing concern in recent years. The rate of emission depends on the fluid mechanics; the fluid can be in the form of a gas, vapor, liquid, or a two-phase vapor–liquid mixture (Figure 3.3). Emission conditions may be categorized as follows: (a) *fluid*, in the form of a liquid and gas or vapor; (b) *oil and gas pipeline infrastructure*, pipe components and equipment; (c) rupture; (d) *enclosure*, in an infrastructure/structure or in an open space; (e) altitude; and (f) fluid momentum.

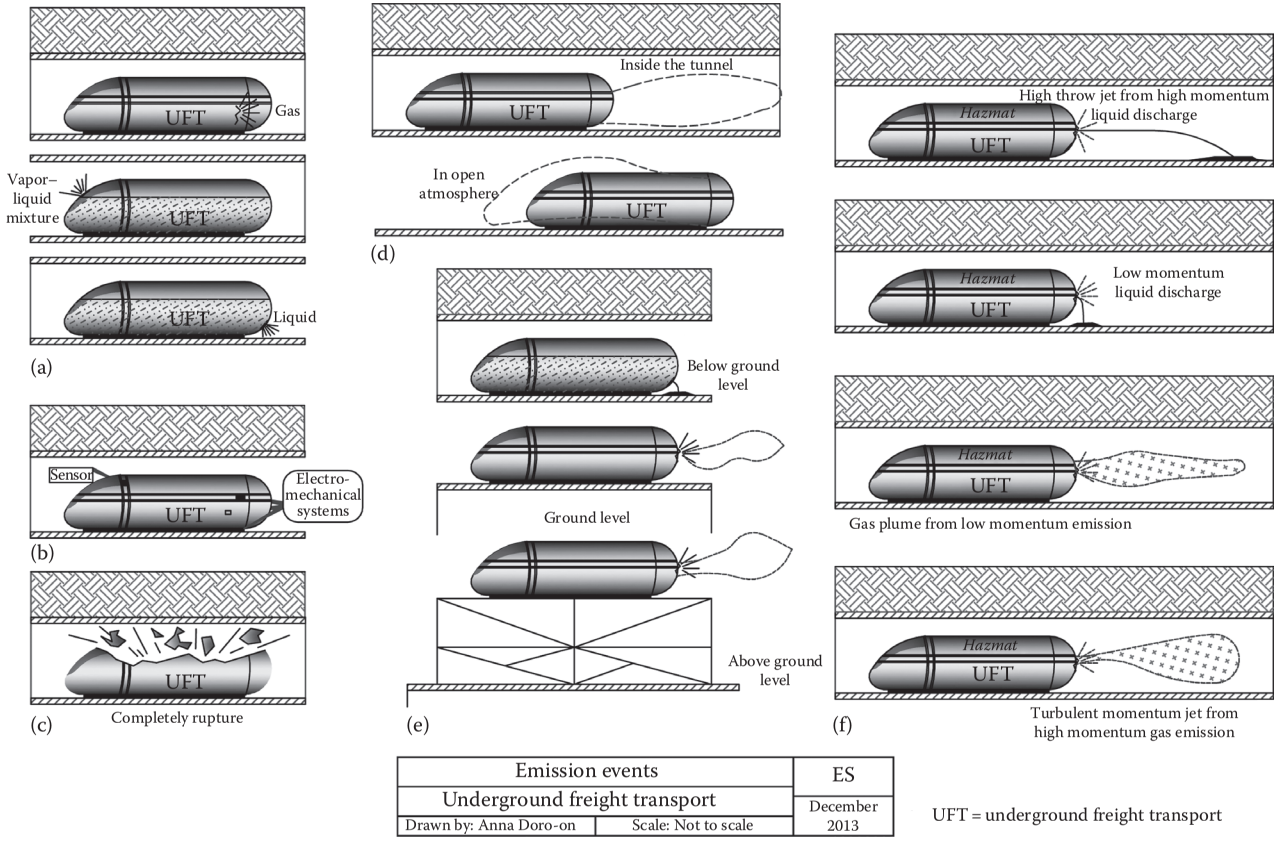


Figure 3.3 Emission events of freight transportation system.

If the emission is coming from a capsulated freight or tank under pressure in a rail transportation holding petrochemical compounds in liquid form with some vapor, the emission will usually be in liquid form if the aperture is below the liquid level. The mass of release is significantly higher for a liquid or vapor–liquid mixture than for a gas or vapor at a designated pressure variance. The vicinity of the oil and gas pipeline in which the release occurs may be a collection tank, large pipe, and other components as shown in Figure 3.3b. The rift where the toxic or flammable fluid release occurs may range from a large fraction of the envelope of the freight capsule in the case of overall to a limited rift such as a hole/crack, as shown in Figure 3.3c. The relief may take place from a structure or in open air, as shown in Figure 3.3d. This largely affects the dispersion of the toxic material. A large proportion of releases in open air are dispersed without incident. The height at which the release takes place also has a strong influence on the dispersion, as shown in Figure 3.3e. A liquid escape from underground freight capsule transportation below ground level may be completely contained. A release of vapor from above the ground surface may be dispersed over a considerable distance. Dispersion is further affected by the momentum of the escaping fluid, as shown in Figure 3.3f. Low and high momentum releases of gas/vapor form a plume and a turbulent momentum jet. Low and high momentum releases of liquid form a liquid stream and a high "throw" liquid jet, respectively, both of which then form a liquid pool. Dispersion of the vapor cloud results from emission and vaporization, whose source may be established or identified as (a) fluid buoyancy; (b) momentum; (c) source geometry; (d) source duration; and (e) source elevation. There are two aspects to why dispersion occurs: (1) meteorological condition (i.e., wind and stability) and (2) topographical condition (i.e., building and obstruction, surface roughness/friction, over urban areas, over coastal and sea areas, over developed areas, and over complex terrain).

3.2.3.1 Dispersion Situation: Buoyancy Effects

There are three conditions of buoyancy:

1. Neutral buoyancy, where the density of the gas–air mixture is near to that of air, or where other gas concentration is low
2. Positive buoyancy, where gases have a small molecular weight and are considered hot gases
3. Negative buoyancy, where most negatively buoyant gases (also known as heavy gases) are produced by HAZMAT

Dispersion of positive, negative, or neutral gases is analyzed separately. Hence, dispersion of gases that do not show positive or negative buoyancy is called passive dispersion.

3.2.3.2 Dispersion Situation: Momentum Effects

A plume is developed that tends to surge when a release of material which has kinetic energy occurs. A momentum jet is generated when the kinetic energy is elevated up to a high level that entrains large quantities of air. The level of air entrainment impacts the cloud density, which is critical to propagate dispersion.

3.2.3.3 Dispersion Situation: Source Terms

A release of material from a pipeline is typically termed as a point source whereas vaporization from a pond or pool is termed as an area source. An immediate short release is known as an instantaneous release and a prolonged release of a material is considered to be a continuous release.

3.2.3.4 Dispersion Situation: Source Elevation

The two categories of classification of source elevation are ground level and elevated level. Release of HAZMAT from a freight transportation accident and release from an oil and gas pipeline explosion can be identified as ground-level sources. Elevated sources are releases from stacks.

3.2.3.5 Dispersion Situation: Meteorology and Topography

Wind direction, speed, and stability are the aspects of meteorology that influence the dispersion of toxic material. Thus, atmospheric stability determines the degree of mixing. The highest dispersion occurs in unstable conditions and less dispersion takes place in stable atmospheric conditions. Normal dispersion in terms of topography happens on flat vegetated area as moderate roughness; other situations are considered very low and very high roughness from dispersion over urban and developed areas (i.e., tall structures), over oceans, and over other dangerous and complicated terrains.

3.2.3.6 Dispersion Situation: Building and Obstructions

Tall infrastructures, buildings, or other obstructions (e.g., trees) in the flow path of the vapor/gas cloud affect its dispersion and flow rate, causing velocity variations and flow distortions. Dispersion in calm conditions occurs during windless skies and nights.

3.2.4 High Toxic Release

High toxic release of chemicals and radioactive material is one of the primary hazards following fire and explosion. The hazard created by toxic material relies on the

type or characteristic of the chemical, range, period of exposure, and situation. A very large release of a toxic material such as depleted uranium with petrochemicals through undesirable events by freight transportation accidents in urban areas is usually considered as a disaster possibly greater than that of fire and explosion. However, a large toxic release is considered less probable to happen often compared to a large fire and explosion. The immediate release of large quantities could generate more casualties and injuries than flammable release. Thus, such extensive release can be more or less lethal depending on the weather condition at the time of release. Lethality normally appears within approximately 20 miles radius from the source point. Hazardous chemicals enter the human body through inhalation, ingestion, and external (physical) contact.

3.2.5 Dust and Fragment Explosion

An explosion is one of the primary causes of hazards. An explosion resulting from sabotage of oil and gas pipelines generates lesser effect than fire but greater than hazardous material release. When it does happen it can highly affect public health and the environment. Nevertheless, an explosion is typically considered a disaster of potentially larger magnitude than fire but less than that of hazardous chemical release.

3.2.5.1 Explosion Process

An explosion is a violent release of physical and/or chemical or nuclear energy in an abrupt manner. The destructive effect of an explosion relies on the rate of energy being released. Physical energy generally develops through the buildup of pressure in gases. For instance, an explosion may derive from a strained freight capsule metal due to high vapor pressure or the sudden rupture of a petrochemical boiler due to brittle fracture. An explosion may emerge from chemical energy due to a chemical reaction (i.e., combustion of flammable vapor). Chemical explosions can be classified either as uniform explosions (e.g., explosion in a tank) or propagating explosions (e.g., explosion in an oil pipeline). Nuclear explosion due to energy release has several distinctions compared to physical or chemical explosions. Nuclear explosion may be thousands of times more violent and powerful depending on the amount of energy release. It only takes a smaller mass of nuclear material to convert into hot, compressed gasses that can result in a large blast wave and a very large proportion of the energy may be emitted in the form of light and heat (i.e., thermal radiation) followed by harmful invisible rays known as nuclear radiation, which will remain over a long period of time. Understanding explosions is essential in infrastructure protection to necessarily (a) estimate or calculate the aftermath of explosions and (b) control production, storage, handling, and transshipment of explosives.

3.2.6 Freight Capsule or Vessel Burst Pressure and Energy Distribution

The higher the pressure, the larger is the explosion in a freight capsule or vessel burst due to overpressure, mechanical failure, and fire engulfment. Pressure relief may fail, which can lead to freight capsule or vessel explosion. Metallurgical corrosion or defect can lead to mechanical failure of a freight capsule prior explosion. If both mechanical and pressure relief are functioning appropriately, capsule or vessel burst may occur due to fire engulfment which originated from the accumulation of pressure. The analysis of energy generated in a freight capsule and vessel burst can be divided into four categories: vessel expansion, vessel rupture, blast, and fragments.

3.2.7 Explosion Destruction by Missiles

Fragments, objects, and sharp debris likely turn into missiles by burst.

3.2.7.1 Sources, Types, and Propagation of Missiles

There are two main classifications of missiles: primary and secondary. A blasting freight capsule or an exploding large vessel generates fragments, which turn into primary missiles. A pathway of blast wave creates secondary missiles. When energy is emitted to objects, which blast off a surface wall due to an internal burst, they are also considered as primary missiles. There are three conditions for primary missiles to occur from a maglev train or high-speed tubular rail burst: (a) bursting into a greater number of small fragments, (b) disconnection and rocketing, and (c) propulsion of one piece (e.g., usually one large part of a maglev train).

3.2.7.2 Number and Size of Missiles

Bursting of freight capsule, maglev train, and mass transit produces a number of missiles that can be dangerous to adjacent infrastructures and the surrounding community. It can be as harmful as a grenade or an improvised explosive device (IED), which can produce a large number of fragments or sharp objects flying as missiles with toxic gas. For a ruptured freight capsule transportation system filled with HAZMAT or flammable liquid/gas, two things can happen: (a) bursting in fragments and (b) breaking up into two objects.

3.2.7.3 Velocity of Missiles

The initial velocity of a missile can be measured by the force exerted on the missile, that is, pressure; the transmission of momentum to the missile; and the transfer of energy to the missile. The amount of pressure or force exerted on a missile depends

on the event or on the surrounding condition. Hence, in the first rupture of a freight capsule containing HAZMAT or flammable fluid, the overpressure may happen due to minimal or high rate of pressures, while the explosion increases the rate of pressure. Blasting of the freight capsule increases shock waves, while gas pressure, ambient pressure, dynamic pressure, and wind exert forces resulting in acceleration of the missiles.

3.2.7.4 Angle of Departure of Missiles

The flight of a missile can be estimated and the angle of departure is required in the process. Moreover, the angle of departure of missiles from a blasting mass transit due to terrorist attacks can be modeled and calculated so that preventive measures may be designed based on the mathematical analysis created. For instance, an ejection of a large piece from the mass transit, the direction of the fuel gas jet, and the angle of departure of one piece are usually delineated. Moreover, this will roughly be the same for both the detachment and propulsion of a ruptured mass transit. The angles of departure in the case of a traveling transit bursting into a large number of fragments are not well characterized. The general postulation is that sharp objects or fragments are projected in uniform distributions in all directions. In addition, the spatial density of the fragments is proportionately greater in the direction of defenseless targets.

3.2.7.5 Shape, Air Resistance, and Flight of Missiles

The shape of the missile in flight affects its behavior. Fragment missiles appear in different shapes, volumes, lengths, and sizes; they could be similar in dimension in all three axes or not so symmetrical. A lift force normal to the trajectory and drag force along the trajectory both act on a missile in flight. A bulky fragment in flight can be described as a drag fragment. Thus, the friction force of the missile in flight is a function of its velocity. The ballistic range is commonly described as the velocity range of projectiles. The resistance is proportional to the velocity when the velocities are less than the ballistic range. The resistance is proportional to the square of the velocity at ballistic level. The function of fluid resistance is difficult to delineate at supersonic velocities. There are three considerations for the flight of a projectile: no air resistance, air resistance proportional to the velocity, and air resistance proportional to the square of the velocity. The “no air resistance” is only used for modeling missiles in flight and not for realistic considerations because it can result in overestimation of velocity and range.

3.2.7.6 Flying Glass

Glass fragments from bursts in rails, underground freight, and high-speed mass transit systems are harmful to passengers and personnel. Features required to model flying

glass fragments are as follows: velocity of glass fragments, breaking force, characteristics of fragment, spatial density and horizontal or range travelled by flying glass.

3.2.7.7 Falling Masonry and Glass

Falling masonry and glass from structural explosions can also be characterized as missiles. People near or underneath the bursting structures are at risk to dangerous missiles. This can generate casualties and severe injuries, and it is vital to estimate the lethality of missiles flying in all directions from the blast. It is important to propose an easement and/or at least a protective measure from the infrastructure or underneath the infrastructure to be utilized as a "safety escape" for public use in the event of an accident, terrorist attack, or disaster. The easement can be used for the density and size distribution of falling missiles or hazardous debris within the allowable distances.

3.3 Underground Freight Transportation through Pipelines, Tubular Rail, and Magnetic Levitation

The increasing demands for the US surface transportation system to facilitate the mobility of people and maintain and improve the productivity of freight services have reached critical conditions in some regions of the nation (Goff et al. 2000). Due to restrictions of right-of-way, environmental mandates, and projected shortfalls in highway revenues, the traditional approach of increasing the capacity of existing highways or developing new highways is often neither pragmatic nor possible (Goff et al. 2000). An integrated transportation system that can provide flexible, convenient, safe, and speedy movement of both people and freight should be developed to satisfy the ever-increasing demands for personal mobility on the one hand and cost-effective, timely, safe, and secure freight transportation on the other (Goff et al. 2000). Some of the underground freight transportation and magnetic levitation systems are presented in Sections 3.3.1 through 3.3.8.

3.3.1 Automated Transportation System

Automated transportation systems (ATS) are modern decentralized driveless transshipment network systems. They can be utilized in urban areas to minimize energy consumption and environmental impact, to retain safety, and to improve quality of life. Another example of an ATS has been built in Morgantown, West Virginia.

3.3.2 Automated Transportation Logistic System

The automated transportation logistics systems (ATLS) can be used efficiently by commercial and industrial facilities for aboveground material and product

distributions controlled by advanced computer systems in monitoring and managing logistics of the network. Typical components include electronically operated cranes, conveyors, sortation, motion/weight sensors, barcodes printing, storage and retrieval systems, and robots. The advantages of ATLS are (a) reduced energy and workforce requirement while maintaining efficiency of logistics distribution; (b) lesser chance of contamination or HAZMAT exposure to workers in a HAZMAT facility; (c) reduced potential errors due to lesser human input needed; and (d) easily managed and operated off-site through programmable logic controls.

3.3.3 Underground Transportation Logistic System

Underground transportation logistics systems (UTLS) are used in mines and tunnel sites. They are similar to ATLS and very effective in overpopulated areas. These technologies can be found in the Netherlands. Land above ground is increasingly limited and expensive in large metropolitan areas so engineers and technology experts are gradually exploring underground infrastructures, optimizing sustainability and energy efficiency, to meet the demands of the public for advanced and fast technologies.

3.3.4 Pneumatic Capsule Pipeline for Underground Freight

European engineers are advancing the reliability and effectiveness of pneumatic capsule pipeline for underground freight (PCPUF) systems. They are focusing on developing and adapting these technologies rapidly for timely distribution of goods in urban areas to drastically reduce traffic and environmental impacts.

3.3.5 CargoCap

CargoCap is an automated capsule transshipment technology developed in Germany for commercial and industrial distribution of goods within urban areas. The main station is located underground and all the components are controlled electronically by programmable logic controls. In the Federal Republic of Germany, roads as a means of transport have reached their limits so that traffic bottlenecks and delays lead to unduly high costs and friction (Stein 2006). Transportation of goods on the streets constitutes a great problem in the development of Germany's economy, especially in congested areas with high density of population and buildings (Schoesser and Stein 2003). Due to the lack of efficiency, the traffic systems including streets, railways, waterways, and aircraft are not able to render trouble-free, safe, and nonpolluting transportation capacities (Schoesser and Stein 2003). Therefore, it becomes necessary to look for new ways of fast, flexible, and on-time handling of traffic processes as well as to create nonpolluting transportation capabilities (Schoesser and Stein 2003). CargoCap is devised as an independent and efficient system, fulfilling operational profitability that can be expanded with

ease (Stein 2006). Transportation as such is effective on the basis of individually driven, computer-controlled transport units (Caps), each of which has a capacity of 2 Euro pallets in accordance with CCG 1 ($B \times D \times H$: $800 \times 1200 \times 1050$ mm) (Stein 2006). Because of underground transportation pipes, CargoCap is independent, unaffected, and uninfluenced by other transports, traffic routes, and traffic jams (CargoCap 2012). Therefore, the assumed lower transport speed, if the transport flow is constant, leads to a significant decrease of transport time in comparison to lorries in congested urban areas (CargoCap 2012). In operation, CargoCap does not impair the environment either with noise or exhaust fumes (CargoCap 2012).

3.3.6 Underground Container and Capsule Transport Systems

A new concept is using underground container transportation systems to distribute containers in ports (Dongjun et al. 2007). According to Kris De Decker (2008), some western European countries are getting serious about transporting consumer goods through automated subterranean networks—introducing a fifth transport mode in addition to road, rail, air, and water. This rare combination of low-tech sense and high-tech knowledge could lead to further economic growth without destroying the environment and the quality of life (De Decker 2008). The most viable techniques, however, adopt just the concept of automated underground transport: they make use of well-known electric propulsion instead of compressed air or electromagnetic forces, and they envision extreme low speeds of 7–35 km/h or 4–22 miles per hour (mph) (De Decker 2008). Germany, Holland, and Belgium are closest to implementing an underground logistics network (De Decker 2008). Trucks are an important cause of noise and air pollution, they cause severe traffic accidents, consume a lot of fuel, and demand a lot of space; however, an automated underground transport system erases all these problems (De Decker 2008). Nowadays, the main research direction is to combine an autotransportation system with an underground tunnel or pipe to construct underground container transportation systems (Zhang and Wang 2011).

Japanese researchers have constructed and tested a prototype linear tube transportation system powered by linear synchronous motors (Tomoji 1994). Linear electric motors belong to a special group of electrical machines that convert electrical energy directly into mechanical energy in the translational motion (McPherson and Laramore 1990). While all electric motors operate based on principles of electromagnetic interactions, there are different types of motors. Polyphase synchronous motors and induction motors both use alternating current as their input electricity source (McPherson and Laramore 1990). There are two choices in using linear induction motors (LIMs) in pipelines (Zhao and Lundgren 2002): (1) one can put primaries of LIMs on the freight capsules. This configuration requires complicated windings on the capsule cart, and electrical current transfers between the traveling capsules and the stationary pipe tubes via some sliding connection.

(2) Alternatively, one can put primary windings on the pipe tubes and build capsules as secondary. The latter configuration makes the system much simpler. If the number of capsules is very small, the second configuration is less efficient than the first one because primaries produce flux without moving the secondary (Zhao and Lundgren 2002). The proposed pipeline transportation concept is envisaged to move a block of capsules at a time (Zhao and Lundgren 2002).

Aerodynamic drag constitutes an important force on a capsule in a pipeline system (Zhao and Lundgren 2002). Based on the Texas Department of Transportation (TDOT; Roop et al. 2000) study, the drag on a capsule by both viscous shear loads and normal pressure loads are itemized as (a) skin friction; (b) pressure drag; (c) shock losses; and (d) rolling resistance. From an aerodynamic perspective, shock losses can be easily reduced by blending the capsule together so that they present a smooth exterior (as is commonly done on high-speed trains) (Roop et al. 2000). The capsule is also assumed to be symmetrically located in the tunnel, which is also of rectangular dimensions (Roop et al. 2000). This drag component is due to viscous shear over the exposed surfaces of the main transportation mechanism (MTM), which is proportional to the square of the MTM speed (Roop et al. 2001). For a given required length of the transportation mechanism, connecting the individual vehicle components to form a continuous surface minimizes skin friction (Roop et al. 2001). In order to offer a viable alternative to truck transportation of freight, the freight pipeline must be able to compete in terms of cost per ton-mile and a significant factor determining cost per ton-mile is the amount of energy consumed by the MTM (Roop et al. 2001). When the MTM reaches the maximum speed, no further acceleration is needed, and therefore the only force required for cruising at this speed is the force to overcome different types of resistances such as the climbing resistance and the aerodynamic drag (Roop et al. 2001). The aerodynamic drag includes skin friction, pressure drag, and shock losses (Roop et al. 2001). In general, the typical pipeline selection parameters include soil types, soil conditions, groundwater, seismic activity, faulting, types of material to be transported, and/or any other special construction requirements (Roop et al. 2000).

A pneumatic capsule pipeline (PCP) uses air blown through a pipeline to propel capsules (wheeled vehicles carrying cargoes) through the pipeline (Liu 2000). All contemporary PCP systems, such as those used in the former Soviet Union for transporting rock (Jvarsheishvili 1981) and those used in Japan for transporting limestone and other products (Kosugi 1992), use wheeled capsules rolling through a pipeline (Liu 2000). The PCP capsules normally have a diameter of approximately 85% of the pipe diameter, and a capsule length of about five times the capsule diameter (Liu 2000). All PCP systems must be automatically controlled and require detection of capsules at many strategic locations along the pipe (Liu 2000). Purdue University (2012) mentioned that the main barrier to long-distance PCP is that the current system is not cost-effective compared to truck and train, which use existing highways and rails, respectively.

3.3.7 Tubular Rail

A train shooting through a series of elevated hoops supported by a suspension system that keeps the rail cars on track (Whaley 2012) is known as a tubular rail. Tubular Rail Inc. (TRI 2011) stated that the tubular rail system is a unique, patented, rapid-transit system that reconfigures traditional rail technology by reversing the orientation of the wheel and the rail. The tubular rail technology (TRT) maintains the same five characteristics of rail transportation but reconfigures them in a highly innovative fashion; it employs the following features (TRI 2012):

- The functionality of the bridge and passenger car is combined. This is accomplished by reversing the orientation of the wheel and the rail. By placing the wheel permanently on a fixed structure and the rail on the now strengthened car, the car itself bridges the space between the rollers.
- TRT uses the principle of the cantilever beam—a projection anchored at one end. As the car is moving within and is held by the support rings, the effect is to create a cantilever beam. The beam is fixed in its vertical orientation but is mobile in its horizontal orientation. Therefore, this rolling cylinder constantly shifts from a cantilever beam on the ends to a post and beam and then back again.

The tubular rail concept would work as a single rigid train that threads the needle through elevated support rings (Hsu 2009). Each train would have guidance rails, and would keep in contact with the electric motors on at least three rings at all times, to reach speeds of up to 150 mph (Hsu 2009). Such O-ring pillars would supposedly represent a huge cost saving compared to laying traditional rail. Robert Pulliam, the Houston resident behind the idea, has assembled a coalition of developers and companies to realize his vision, and hopes to raise $30 million for a 2 or 3-mile test track (Hsu 2009).

3.3.8 Magnetic Levitation Transportation System

Magnetic levitation (Maglev) is a completely new mode of high-speed transport vehicle, which is lifted by magnetic repulsion and propelled along an elevated guideway by powerful magnets attached to the vehicle (Powell and Danby 2005). As the guideways are elevated, there is no possibility of collisions with autos or trucks at grade crossings (Powell and Danby 2005). A Maglev transport system includes magnetic levitation vehicles each driven by a linear motor to run along the truck (Shibata and Murayama 1995). Each vehicle includes electromagnets to attract levitating magnetic members extending along the running track, a pickup coil resonant with a frequency of the induction lines to generate an electromotive force, and a battery chargeable by the pickup coil (Shibata and Murayama 1995). The electromagnets receive power from the pickup coil and/or the battery (Shibata and Murayama 1995).

The US National Aeronautics and Space Administration (NASA 2012) stated that Maglev, which was developed by Transrapid International in Germany, has conventional iron-core magnets in the vehicle's wraparound arms that are pulled up to magnets under the guideway. A relatively small air gap (1 cm) separates the vehicle and guideway magnets (NASA 2012). Although not part of the present Transrapid design, superconducting magnets can be incorporated in attraction-type Maglev systems (NASA 2012). According to Iran Maglev Technology (IMT 2012), Maglev has various cases, including clean energy (small and huge wind turbines: at home, office, industry, etc.), building facilities, transportation systems (magnetically levitated train), weapon (gun and rocketry), nuclear engineering (the centrifuge of nuclear reactor), civil engineering (elevator), advertising (levitating every character inside or above various frames can be selected), and so on. The common point in all these applications is the lack of contact and thus no wear and friction (IMT 2012). This increases efficiency, reduces maintenance costs, and increases the useful life of the system (IMT 2012). The need for rapid transit systems has become vital in both urban and intercity travel (Yaghoubi 2011).

One of the first major applications of magnetic levitation was in supporting airplane models in wind tunnels (Yaghoubi 2012). Researchers had found that mechanical support structures sometimes interfered with airflow enough to produce drag more than the drag force on the model (Yaghoubi 2012). The solution developed by Gene Covert and his MIT colleagues in the 1950s was magnetic levitation (although they called it a "magnetic suspension and balance system") (Yaghoubi 2012). About 20 years later, Werner Kemper of Germany proposed a train magnetically levitated by a feedback-controlled attractive force, and after many decades of development, it eventually evolved into the Transrapid system used in the Shanghai Maglev train in 2003 (Yaghoubi 2012). Maglev systems represent an entirely new concept in transportation (Sandberg and Williams 2010). The high cost of constructing a Maglev system demands that special attention be given to planning for future growth (Sandberg and Williams 2010). Thus, there have been no specific studies detailing disasters related to Maglev transportation systems.

3.4 Railroad and Railway Systems

Railroad and railway systems are designed for transshipment of passengers, goods, and other type of freight systems. Railroad is largely used in the United States for hauling operations. On the other hand, railway is the most preferred modern terminology of railroad in urban and interurban rail transportation systems. With the introduction of the steam locomotive in 1829, a mechanized land transport system became available for the first time (Rodrigue and Slack 2012). For instance, Burlington Northern Santa Fe (BNSF) Railway is the outcome of some 390 different railroad lines that merged or were acquired over a period of more than 150 years

(Rodrigue and Slack 2012). The railway started being built and used in the seventeenth century for carrying coal. Cart wheels made of wood were equipped to operate on short timbers laid on crossties. The surface of these timbers was protected by strips of wrought iron, which were subsequently substituted by cast-iron rails with an inner flange (Haines 1919). In 1789, these were replaced by the "edge-rail" and the flanged wheel, and the modern railway was born (Haines 1919).

The advent of the railway era really dates from the charter of the Stockton & Darlington Railway Company in 1821 (Haines 1919). It was on this railway, after 20 miles of the line had been worked on by horsepower, that Stephenson operated his engine, "Locomotion No.1," in 1825 (Haines 1919). The locomotive was originated in 1829 by George Stephenson, who brought the multitubular boiler and the exhaust draft for the rail system. In the United States, the beginning of the development of the locomotive dates from almost the same time as in England. Railway transportation in England was introduced into populous regions with large volumes of traffic (Haines 1919). Railroads in the United States were constructed in remote environments. As the country was virtually devoid of roads, the railroads preceded them; in fact, they preceded civilization (Haines 1919). They were not intended to care for existing traffic, but to create it and populate vast uninhabited areas, for they were extended into regions still in a primitive state, verging on barbarism (Haines 1919). The operation of the first steam-drawn train started and evolved over more than 100 years, which made a significant contribution to the economic environment and methods that existed in the previous 10,000 years. Railways provided job opportunities, so that workers were recruited from occupations where skills were roughly analogous and transferable, that is, workshop mechanics from the iron, machine, and building trades; conductors from stagecoach drivers, steamship stewards, and mail boat captains; station masters from commerce and commission agencies; and clerks from government offices (Licht 1987). In parallel with the expansion of railroads in the entire country after the Civil War, the death toll and rate of injuries due to accidents increased among railroad workers. Most of these accidents were related to the operation of hand brakes and manually operated railroad vehicles. The rise in accidents led to calls for a safety legislation, as early as the 1870s (McDonald 1993). In the 1880s, the number of on-the-job fatalities of railroad workers was second only to those of coal miners. Through that decade, several state legislatures enacted safety laws (McDonald 1993). However, the specific requirements varied among the states, making implementation difficult for interstate rail carriers, and Congress passed the Safety Appliance Act in 1893 to provide a uniform standard (McDonald 1993). The Esch–Cummins Act of 1920 terminated the nationalization program and created a Railway Labor Board (RLB) to regulate wages and issue nonbinding proposals to settle disputes. In 1921, the RLB ordered a 12% reduction in employees' wages, which led to the Great Railroad Strike of 1922, involving rail shop workers nationwide, followed by a court injunction to end the strike (David 1997). According to the United States Code Title 45 USC § 151 (1926), Congress

passed the Railway Labor Act of 1926 to rectify the shortcomings of the RLB procedures. Freight rail transport is widespread and heavily used in North America, but intercity passenger rail transport on that continent is relatively scarce outside the Northeast Corridor due to the loss of competition to other preferred modes, particularly automobiles and airplanes (EuDaly et al. 2009). As opposed to highway expansion, indicative of the US transportation policy, rail transport incentivizes the development of suburbs at the periphery, contributing to increased vehicle miles traveled, carbon emissions, development of Greenfield spaces, and depletion of natural reserves, railways channel growth toward dense city agglomerations and along its artery. These arrangements revalue city spaces, local taxes, housing values, and promotion of mixed-use development (Squires 2002).

3.5 Oil, Gas, and Other Hazardous Liquid Pipelines

There are two common types of energy source pipelines: oil pipelines and gas (also known as natural gas) pipelines. Generally, people relate *pipelines* with water utilities or storm water systems as they often see in the surrounding areas. Also, most of us will have seen the plastic pipes laid under our streets and roads to locally distribute natural gas (Hopkins 2007). But what many people do not know is that there are hundreds of thousands of kilometers of very large pipelines crossing our nations and oceans transmitting huge quantities of crude oil, oil products, and gas. Most are underground or undersea: out of sight, out of mind (Hopkins 2007). Oil and gas pipelines have been among the biggest infrastructure projects in developing countries in recent years (Goodland 2005). Nearly 30,000 km of pipelines are planned annually for the following years (Goodland 2005). The fuels providing the world with its primary energy needs are oil = 34%, coal = 24%, gas = 21%, nuclear = 7%, hydro = 2%, and others = 12% (Hopkins 2007). These high-pressure large-capacity pipelines carry hazardous products and, consequently, are designed, constructed, and operated using recognized standards that all focus on safety (Hopkins 2007).

Petroleum or crude oil is a naturally occurring flammable liquid formed beneath the Earth's surface and extracted by oil drilling through 2–8 in. in diameter *gathering lines*. It is distributed through large (8–48 in. in diameter) *trunk lines* from producing areas to refineries. A similar process of petroleum is used for natural gas, where gathering lines are utilized to extract gas and impurities are removed by natural gas-processing plants. According to Pipeline 101 (2007), there are about 20,000 miles of natural gas gathering lines. The gathering lines move natural gas to large cross-country transmission pipelines (Pipeline 101 2007). The US Energy Information Administration (EIA 2001) stated that more than 165 US intra- and interstate natural gas pipeline companies operate about 278,000 miles of transmission lines, hundreds of compressor stations, and numerous storage facilities, allowing gas delivery throughout the lower 48 states. Oil moves through pipelines at speeds of 3–8 mph (Trench 2001). Based on the Argonne National Laboratory

(2007) information, there are approximately 55,000 miles of crude oil trunk lines (usually 8–24 in. in diameter) in the United States that connect regional markets. The United States also has an estimated 30,000–40,000 miles of small gathering lines (usually 2–6 in. in diameter) located primarily in Texas, Oklahoma, Louisiana, and Wyoming, with small systems in a number of other oil-producing states. These small lines gather the oil from many wells, both onshore and offshore, and connect to larger trunk lines measuring 8–24 in. in diameter (ANL 2007). Natural gas provides over 25% of residential and industrial energy needs, while oil products provide 97% of the energy used for transportation (Technical Support Working Group [TSWG] 2011). In total, 62% of the energy used in the United States is derived from these two sources (DHS 2007). Over the past 2 years, more than 60 natural gas pipeline construction projects (35 in 1999 and 28 in 2000) have been completed and placed in service in the United States, accounting for more than 12.3 billion cubic feet per day of new pipeline capacity, an increase of 15% over the capacity level in 1998 (EIA 2001). The ability to store natural gas is essential to the operation of the natural gas market. Withdrawals from storage provide additional gas supply during seasonal and short-term gas demand peaks, help keep pipelines and distribution systems in physical balance, and play an important role in commodity trading and management (EIA 2001). The American Society of Mechanical Engineers (ASME) has a long history of developing standards for use in the oil and gas pipelines industry (ANL 2007). As the needs of the industry evolved over the years, rules for new construction have been enhanced, and rules for operation, inspection, corrosion control, and maintenance have been added (ANL 2007). Table 3.1 presents some of the large pipelines, failure, disaster, and terrorism.

3.5.1 Unregulated Hazardous Material Liquid Pipelines

About 240,000 miles of pipelines ferry oil and natural gas from wells to refineries across the United States, and amid a boom in natural gas the network continues to grow (Malewitz 2012). The use of pipelines is largely seen as the safest way to carry oil and natural gas, killing hundreds fewer people each year when compared to transport by freight trucks or trains (Malewitz 2012). Most unregulated pipelines operate at lower pressures and away from population centers, but they still present safety risks, state regulators say, particularly as increased shale drilling sparks development across pipelines' right-of-way (Malewitz 2012).

In general, Pipeline and Hazardous Materials Safety Administration (PHMSA) administers the national regulatory program to ensure the safe transportation of hazardous liquid and gas through pipelines (GAO 2012). PHMSA performs its oversight role using uniform, minimum safety standards that all pipeline operators regulated by PHMSA must meet, as well as a supplemental risk-based regulatory program termed "integrity management" for pipelines in "high-consequence areas" where an incident would have greater consequences for public safety or the environment (GAO 2012). While gathering pipelines generally pose lower safety risks

than other types of pipelines, PHMSA does not collect comprehensive data on safety risks associated with gathering pipelines (GAO 2012). Operators of unregulated gathering pipelines are not required by federal law to report information on such risk factors (GAO 2012). PHMSA is currently not able to determine the performance and safety of these gathering pipelines because it does not collect the necessary pipeline operator data (GAO 2012). The absence of information sharing resources focused on federally unregulated gathering pipelines means that both states and PHMSA could miss opportunities to share lessons learned and successful practices for helping to ensure pipeline safety (GAO 2012).

Most commonly reported concerns are with limited information about unregulated pipeline construction quality (DOT-PHMSA 2013). According to DOT-PHMSA (2013), PHMSA is currently considering regulating these gathering pipelines. The lines being put into service in the various shale areas like Marcellus, Utica, Barnett, and Bakken are generally of much larger diameter and operating at higher pressure than traditional rural gas gathering lines, increasing the concern for the safety of the environment and the people near operations (DOT-PHMSA 2013). Data collected about these new gathering pipelines would contribute to a body of public knowledge enabling safer and more reliable pipeline operations. Due to the recent GAO report in 2012, PHMSA has been mobilized and is in the process of collecting data on unregulated pipelines. They recently acknowledged the growing concerns of unregulated pipelines. But due to a lack of reasonable amount of data related to hazard and man-made disaster on these unregulated pipelines, enforcing safety and security for these pipelines was delayed.

3.6 Underwater/Immersed Tunnel and Cross-River Tunnel

Marc Isambard Brunel, a French tunnel engineer, developed, patented, and applied the first underwater tunnel technology, called the "tunneling shield," with Lord Cochrane in 1818. One of the famous projects where he used his technology was to build and construct the underwater Thames Tunnel in the United Kingdom. Another famous modern underwater tunnel is the Ted Williams Tunnel (TWT) located under Boston Harbor in Boston, Massachusetts. The TWT is 8448 ft long and more than one-third of its length is underwater. The world's largest dredging vessel, the *Super Scoop*, which is owned by the Dutra Group, was used to dig a 50-ft-deep, 100-ft-wide trench for three-quarters of a mile beneath Boston Harbor. Workers dug the trench to accommodate the 12 immersed tube tunnel (ITT) sections that would comprise the main underwater tunnel (Eastern Roads 2012). The first of the 12 ITT sections arrived in the Reserve Channel in September 1992 (Eastern Roads 2012). Each of the twin-tube tunnel sections measures 325 ft long and weighs 7500 tons. Each tube within the ITT section has a diameter of 40 ft, enough to accommodate two traffic lanes (Eastern Roads 2012). The ITT sections

were prefabricated at the Bethlehem Steel shipyard in Baltimore, and sent by barge at a rate of one a month 400 miles north to the tunnel site at Black Falcon Terminal (Eastern Roads 2012).

Recently, Russia and the United States agreed to build the longest underwater tunnel between Russia and Alaska, United States. Tiffany Gabbay (2011) described how the United States and Russia have cooperated in space, and now the two countries are adding high seas to the mix, having set their minds on connecting the Eurasian and American continents via underwater tunnels in the Bering Strait. The Bering Strait lies just south of the Arctic Circle and is subject to long, dark winters and extreme weather (average lows of –4°F or –20°C) with extreme lows approaching –58°F (–50°C) and high winds (Ricci 2012). Connecting the continents with a bridge or tunnel would represent an extraordinary engineering feat (Ricci 2012). A tunnel would be nearly twice as long as the Chunnel, the 31-mile-long tunnel that connects England and France (Ricci 2012). The Russian International Affairs Council (RIAC 2012) pointed out that the idea to connect Eurasia and North America via the Bering Strait is not a new one. Russia had already started tackling it at the end of the nineteenth century after the construction of the Trans-Siberian railroad, but even with the approval of Nicolas the Second and key ministers, this project didn't reach the implementation stage in the last years of the tsarist Russia or after October 1917 as the country was faced with more important tasks at that time (RIAC 2012).

Another type of underwater tunnel is known as the *cross-river tunnel*, which is a tunnel or tunnels constructed underneath a river to connect aboveground areas, normally used for rail network and transportation systems. Nanjing, the capital of Jiangsu Province on the east coast of China, is constructing a second highway tunnel crossing the Yangtze River also known as *cross-river tunnel of the Yangtze River* (Long 2011). The cross-river project is an integral component of an overall plan that is being delivered using the build–operate–transfer model (Long 2011). The Chinese project faces many challenges such as (Long 2011) (a) complex geological conditions, because the traditional cutter bits for soft soil and disc cutter for hard rock are, in some senses, incompatible; (b) high water pressure, where water pressure is approximately 7.7 bar, which requires special design of the brush tail seal and the main bearing seal, and the development of a system for replacing tools under normal atmospheric pressure; (c) long-distance drive, which may result in high wear of the cutter-head tools; and (d) simultaneous construction of the interior structure, which will require careful planning to synchronize the many interrelated works.

Shanghai is one of the biggest cities in China, and the density of buildings is quite high (He et al. 2008). In 2002, Shanghai built its first double-o-tube shield in No. 8 line (He et al. 2008). Fuxing Donglu cross-river tunnel, a double-o-tube and deck, is rated as China's first of its kind (People Daily 2002). Double tube and deck means that in a tunnel two tubes are designed according to the to-and-fro direction of traffic movement and each tube is divided into two decks (People Daily 2002). Another example of a proposed new cross-river tunnel is the Cross-River Rail project in Brisbane, Australia. In July 2012, Cross-River Rail's *ready-to-proceed*

status was reconfirmed by infrastructure Australia on their National Priority list of projects (Queensland Government 2012).

3.7 Transportation Tunnels

It is estimated that there are 337 highway tunnels and 211 transit tunnels in the United States (AASHTO 2003). These tunnels move thousands of people and tons of cargo daily (TCRP 2006). Many of these tunnel facilities are located at key *choke points* in the nation's transportation network (TCRP 2006). Tunnels can face disruption either from the occurrence of hazards (i.e., unintentional, accidental events) or from the successful conduct of threats (i.e., intentional acts) (TCRP 2006). Hazards can be human- or equipment-related (e.g., motor vehicle collisions and resulting fire) or natural causes (e.g., flooding and earthquakes) (TCRP 2006). From a policy perspective, tunnel managers have two significant concerns. First, tunnels serve important day-to-day transportation functions, often providing nonredundant network connections (TCRP 2006). Second, owners must plan for effective use of the tunnels to transport people and goods as emergency relief in the event of severe emergencies occurring elsewhere (TCRP 2006). This section focuses on three kinds of transportation tunnels: highway/road, rail, and transit. Rail (which includes both passenger and freight) and transit tunnels are separate categories (TCRP 2006).

3.7.1 Road Tunnels

The United States Department of Transportation–Federal Highway Administration (DOT-FHWA 2009) stated that road tunnels, as defined by the American Association of State Highway and Transportation Officials (AASHTO) Technical Committee for Tunnels (T-20), are enclosed roadways with vehicle access that is restricted to portals regardless of type of the structure or method of construction. Road tunnels are feasible alternatives to cross a water body or traverse through physical barriers such as mountains, existing roadways, railroads, or facilities; or to satisfy environmental or ecological requirements (DOT-FHWA 2009). The design of the horizontal and vertical alignment of a road or highway section, which includes a tunnel, constitutes a major and fundamental first stage in the creation of a new tunnel, to which the necessary attention is seldom given (WRA-PIARC 2011). A certain number of parameters have a major impact from the upstream stages of the project onward and they must be analyzed from the first phases of the design and deal in particular with (a) volume of traffic, nature of the traffic (urban, nonurban), nature of vehicles (possibly tunnel dedicated to one category of vehicles), and transport or not of dangerous goods; (b) evacuation of the users and access of the emergency teams; (c) ventilation; and (d) communication with the users and supervision system (WRA-PIARC 2011). Traditionally, tunnels are

designed for a life of 100–125 years (DOT-FHWA 2009). However, old existing tunnels (over 100 years old) still operate successfully throughout the world and have been used to design tunnels for 150 years life (DOT-FHWA 2009).

The principal types and methods of tunnel construction that are in use are (DOT-FHWA 2009)

- Cut-and-cover tunnels, built by excavating a trench, constructing the concrete structure in the trench, and covering it with soil
- Bored or mined tunnels, built without excavating the ground surface
- Rock tunnels, excavated through the rock by drilling and blasting, by mechanized excavators in softer rock, or by using rock tunnel boring machines (TBM)
- Soft ground tunnels, excavated in soil using a shield or pressurized face TBM, or by mining, known as the sequential excavation method (SEM)
- Immersed tunnels, made from very large precast concrete or concrete-filled steel elements that are fabricated in the dry, floated to the site, placed in a prepared trench below water, connected to the previous elements, and then covered up with backfill
- Jacked box tunnels, prefabricated box structures jacked horizontally through the soil using methods to reduce surface friction

Highway requirements for road tunnels vary according to the tunnel situation and character (urban, interstate, subaqueous, or mountain), and whether they are long or short (DOT-FHWA 2004). There are two main considerations for tunnel operations (DOT-FHWA 2004): (a) tunnels with their own dedicated operating management structure and resources, which retain responsibility for traffic surveillance and safe operation of the tunnel, including response to incidents and emergencies; and (b) tunnels designed to operate as fully automatic facilities, with no permanent operating and monitoring staff, which allow free passage of dangerous goods vehicles operating within the law.

The nature and mix of vehicles in the traffic flow will also affect the physical design of tunnels (DOT-FHWA 2004). For *interstate highway tunnels*, tunnel line and gradients should conform to standards specified for the interstate: sight lines appropriate to the design speed should require particular care, especially where vertical curves are necessary (DOT-FHWA 2004). Design speed should be greater than 60 mile/h (97 km/h), unless otherwise restricted in urban areas; and the minimum radius of curvature should not be less than 1500 ft (457 m) (DOT-FHWA 2004).

3.7.2 Transit and Rail Tunnels

Tunnels were considered unique structures and special applications would be needed for them (DOT-FHWA 2005). Transit tunnels and underground structures are vital links in the metropolitan economic system that represent enormous

long-term public investments by the communities, municipalities, and regions they serve (TCRP 1997). Rail transit tunnel design is affected by several factors, which, if inadequately assessed, may have adverse impacts on subsequent inspection: the intended and actual use of a tunnel, the physical conditions within which a tunnel is constructed, and the construction materials used in a tunnel that affect both the types and frequencies of tunnel inspection (TCRP 1997). The shape of rail transit tunnels often varies along a given rail line (DOT-FHWA 2005). These shapes typically change at the transition between the station structure and the tunnel cross section (DOT-FHWA 2005). While transit capacity issues are mainly concentrated in larger cities, transit quality of service is important to all communities. Transit quality-of-service measures reflect two important aspects of transit service: (1) the degree to which transit service is *available* to given locations and (2) the *comfort and convenience* of the service provided to passengers. Quality-of-service measures differ both from traditional highway service quality measures, which are more vehicle-oriented than person-oriented, and from the numerous utilization and economic performance measures routinely collected by the transit industry, which tend to reflect the transit operator's point of view (TCRP 2003).

The nation's growth and the need to meet mobility, environmental, and energy objectives place demands on public transit systems (TCRP 1997). Transit plays two major roles in North America. The first is to accommodate *choice* riders—those riders who choose to use transit for their trip-making even though they have other means of travel, in particular, a motor vehicle (TCRP 2003). The other major role of transit is to provide basic mobility for those segments of the population too young, too old, or otherwise unable to drive due to physical, mental, or financial disadvantages (TCRP 2003). Transit systems carry a majority of all peak-hour travelers to the downtown areas in many older major North American cities, but in other metropolitan areas, they carry a smaller proportion of downtown trips (TCRP 2003).

3.8 Mine Tunnels

Mine tunnels are created similar to other tunnel systems but they are built with fewer resources and less funding is required. A mine tunnel is used for access to lode mining claims or to explore for blind or undiscovered veins, lodes, or ledges not currently claimed or known to exist on the surface and can be up to 3000 ft in length (BLM 2012). The California Department of Industrial Relations (DIR 2012) defined mining as any excavation or opening above or below ground used for removal of ore, minerals, gravel, sand, rock, or other materials intended for manufacturing or sale. It shall include quarries and open pit operations, other than a gravel pit or other pit where material is removed by a contractor or other person for his or her own use and not for sale to others (DIR 2012). Underground mine means a mine that consists of a subterranean excavation (DIR 2012). Mine tunnels create a

network of tunnels that extend for many miles, at different elevations below ground surface and typically constructed with timber, concrete, and steel, and considered to be extra-hazardous compared to other tunnel systems. Most mine disasters are generated by earthquakes or geotechnical stress. On August 16, 2012, in the Democratic Republic of Congo, at least 60 miners died from mine shaft collapse. The mine tunnels collapse in China generated approximately 2600 deaths in 2010. Due to the stringent regulations for mine workers safety in the United States, there are fewer casualties caused by mine tunnels collapse compared to other countries.

3.9 Drainage Tunnels

A drainage tunnel is designed and constructed to discharge treated liquid waste from underground mines or storm water. Most drainage tunnels for storm water diversion in large urban or metropolitan areas are typically 20–30 ft in diameter and several miles in length (i.e., 5 miles minimum). The engineering design requirement of drainage tunnels in urban areas is dictated by flood water flow rates based on the flood protection standards given by the state or local government.

3.10 Aqueducts

Another unique pipeline system in the United States comprises *aqueducts*, which are currently facing a deficiency in security systems. Aqueduct pipelines are large water conveyors considered to be the *life blood* of the two largest metropolitan areas, the leading agriculture producer in the United States, and the leading entertainment industry in the entire world: New York, Central California, and Los Angeles.

3.11 Defense and Warfare Tunnels

Tunnel systems are also used and constructed for defense and warfare. In 1965 during the Vietnam War, the base area at Cu Chi District was a vast network, with nearly 200 miles of tunnels (PBS Press 2012). Any facility used by the guerillas—a conference room or training area—had almost immediate underground access (PBS Press 2012). Soldiers used these underground routes to house troops, transport communications and supplies, lay booby traps, and mount surprise attacks, after which they could disappear underground to safety (History 2012). In modern days, tunnels are preferably used for secret legal or illegal transport, storage, and operations for defense and warfare. According to Anthony Cordesman (1999), Iran has created underground shelters and tunnels in its coastal areas which it could use to store Scud and other missiles in hardened sites, thus reducing their vulnerability to air attack. There are three types of tunnels constructed in this project: tunnels

constructed in mountains, underground tunnels, and aboveground tunnels: (a) tunnels are excavated in mountains to a certain distance and then branch out into several tunnels; (b) underground tunnels are constructed vertically into the ground and branch out at a certain depth; and (c) aboveground tunnels are constructed on the ground and after completion of the support structure, they are covered with earth and camouflaged to resemble terrain features such as hills (Iran Nuclear 2005). Some of these tunnels consist of tens of thousands of square meters of facilities including command and work sections, research workshops, weapons development section, air conditioning and central heating systems, and systems to prevent leakage of radiation and sound to the environment (Iran Nuclear 2005). A special lead lining is used in the tunnels to stop any kind of leakage of radiation and sound to the surrounding environment to prevent detection through soil or other environmental samplings on the ground (Iran Nuclear 2005). The tunnel construction project is primarily under the direction of Iran's Revolutionary Guards Corps (IRGC) and the Defense Ministry, based on the press conference by Mr. Mohammad Mohaddessin, Chairman of the Foreign Affairs Committee of National Council of Resistance of Iran (Iran Nuclear 2005). An underground tunnel system in the Haft-Tir military complex in Isfahan (central Iran) is currently being constructed by a company called Pars Garma (Iran Nuclear 2005). A tunnel complex has also been constructed in the Parchin site (east of Tehran) and is used to conceal nuclear equipment, and one of the tunnels in this particular complex is used to conduct research into laser techniques for uranium enrichment (Iran Nuclear 2005). An extensive tunnel complex used to build ballistic missiles with nuclear warheads is located in the Khojeer region in southeast Tehran (Iran Nuclear 2005). One of these tunnels is for the final assembly of ballistic missiles and is 1000 m long and 12 m wide and the tunnel subsequently branches to five other 500-m-long tunnels (Iran Nuclear 2005). Heavily mountainous Iran has a long history of tunneling toward civilian as well as military ends, and Mahmoud Ahmadinejad has played a recurring role—first as a transportation engineer and founder of the Iranian Tunneling Association and now as the nation's president (Broad 2010). Mr. Ahmadinejad began his professional life as a transportation engineer with close ties to the Revolutionary Guards and an abiding interest in tunnels (Broad 2010). The United Nations atomic inspectors did check out a few of the tunnels at Isfahan, but not at Qum because the plant was on a military base and thus off limits for inspection without strong evidence of suspicious activity (Broad 2010). In early 2004, while he was the mayor of Tehran, Mr. Ahmadinejad served as chairman of the Sixth Iranian Tunneling Conference (Broad 2010). Iran's use of a complex web of tunnels goes back more than a decade and may be the source for the construction of a similar network by Hizbullah in southern Lebanon and by Hamas under the border between Egypt and Gaza (Gedalyahu 2010).

A secret bomb-proof tunnel network reported by Al Jazeera (2009) is being constructed by Myanmar and North Korean engineers as a military complex, which has between 600 and 800 underground facilities and tunnels in various

stages of construction. The tunnel project, reportedly given the codename *Tortoise Shells* by Myanmar's military, is believed to have been implemented with North Korean involvement between 1996 and 2006 (Al Jazeera 2009). The tunnel network which the DVB says was disguised as a fiber-optic cable installation project had enough food and room for about 600 people to survive underground for several months (Al Jazeera 2009). The Myanmar delegation also reportedly inspected North Korean arms factories and later officially formalized military cooperation between the two countries (Al Jazeera 2009). Further, North Korea is digging up a new underground tunnel at the Punggye-ri nuclear test site, in addition to its existing two underground tunnels, and it has been confirmed that the excavation work is in the final stages (Demetriou 2012). Meanwhile, North Korea took the unusual step of inviting foreign journalists into the secret region in order to view its rocket launch site in a bid to convince the world of its argument that its intentions are peaceful (Demetriou 2012).

China has secretly built a major underground nuclear submarine base that could threaten Asian countries and challenge American power in the region, which can be disclosed (The Telegraph 2008). Recently, a Georgetown University professor and his students stirred up a controversy within the US scientific community with a study they say indicates that China may be hiding between 2000 and 4000 nuclear weapons in underground tunnels (Presutti 2011). Scientists and nuclear activists are livid about the conclusions made here at Georgetown. They say Professor Karber's work lacks credibility and thorough research (Presutti 2011). The blogs quoted this 1995 article from Hong Kong that quotes China's defense ministry as stating that it has 2350 nuclear warheads, based on PRC data (Presutti 2011). But the scientists say the article is questionable and have an issue with Professor Karber's students for not tracing their information back to its original source (Presutti 2011).

3.12 Illegal Underground Tunnels

Legislation that would broaden the scope of tactics used to eradicate illegal underground tunnels that traverse the US–Mexico border would also put more responsibility on property owners to report suspicious activity (Aguilar 2012). Of the 149 cross-border tunnels found since 1990, 139 have been found since 2001, according to the bill (Aguilar 2012). Though the problem has largely been confined to Arizona and California, a 130-ft-long passageway was discovered in El Paso in 2010 (Aguilar 2012). As US authorities heighten enforcement on land, tunnels have become an increasingly common way to smuggle enormous loads of heroin, marijuana, and other drugs into the country (Associated Press 2012). The latest Arizona tunnel was discovered after state police pulled over a man who had 39 lb of methamphetamine in his vehicle and mentioned the strip mall (Associated Press 2012). The tunnel was found beneath a water tank in a storage room and stretched across the border to an ice plant business in the Mexican city of San Luis Rio, Colorado,

and it takes 6 months to 1 year to build a tunnel, authorities say (Associated Press 2012). In foreign countries such as in India, an illegal 400-m-long tunnel was found between India and Pakistan, along the International Border in Samba district of Jammu and Kashmir (Pakistan Defence 2012). The tunnel, of 3×3 ft, was detected after an area caved in at two or three places due to rains (Pakistan Defence 2012). Major General (retired) G.D. Bakshi has said that Pakistan has copied the concept of secret tunnels from North Korea with an aim to infiltrate Jammu and Kashmir and spread militancy (The Indian Express 2012). Bakshi also mentioned that a campaign for uncovering such tunnels by the paramilitary Border Security Force (BSF) should be top priority (The Indian Express 2012). Moreover, the Israel Ministry of Foreign Affairs (2012) pointed out that there are 100 terror sites being targeted, including dozens of terror infrastructure sites throughout the Gaza Strip.

3.13 Implication

Illegal secret tunnels and terrorism on freight capsule pipelines, underground high-speed rail, and transit systems could negatively affect public safety, capital assets, socioeconomic stability, and even national security. The only way to determine the requirement levels of protection and defense is to utilize risk assessment and risk acceptability analyses based on quantitative psychology, so that stronger deterrent technologies can be employed effectively. Chapters 4, 5, and 7 demonstrate different types of risk assessment methodologies and acceptable risk measures for infrastructure and homeland protection. Further, Chapter 7 presents more detailed graphical illustrations related to this chapter with comprehensive risk analyses, and provides information related to military support for civilians in the event of terrorist attacks or WMD detonation.

References

Aguilar, J. 2012. Bill would bolster efforts to stop clandestine tunnels. http://www.texastribune.org/texas-mexico-border-news/texas-mexico-border/bill-would-bolster-efforts-stop-clandestine-tunnel/ (accessed on June 2, 2012).

Al Jazeera. 2009. Myanmar's secret tunnels' revealed: Report says North Korean engineers building underground military complex. http://www.aljazeera.com/news/asia-pacific/2009/06/20096255353936689.html (accessed August 2, 2012).

American Association of State Highway and Transportation Officials (AASHTO). 2003. Recommendations for bridge and tunnel security, Transportation Security Task Force, The Blue Ribbon Panel on Bridge and Tunnel Security. http://www.fhwa.dot.gov/bridge/security/brp.pdf (accessed December 1, 2012).

Argonne National Laboratory (ANL). 2007. Overview of the design, construction, and operation of interstate liquid petroleum pipelines. http://corridoreis.anl.gov/documents/docs/technical/APT_60928_EVS_TM_08_1.pdf (accessed June 12, 2012).

Associated Press 2012. US-Mexico Border Tunnel Nets 40 Tons of Pot. Editors-J. Billeaud and E. Spagat; http://www.ldnews.com/national/ci_21066463/2-sophisticated-border-drug-tunnels-discovered (accessed September 2, 2012).

Badkar, M. 2012. 15 countries sitting on gigantic oceans of oil. http://www.businessinsider.com/15-countries-with-the-biggest-oil-reserves-2012-4?op=1 (accessed September 2, 2012).

Ballantyne, D. 2008. Oil and gas pipelines, US Geological Survey Open File Report 2008-1150, California Geological Survey Preliminary Report 25 version 1.0. http://www.colorado.edu/hazards/shakeout/pipelines.pdf (accessed December 1, 2012).

BP Energy. 2011. Statistical review of world energy. http://www.bp.com/liveassets/bp_internet/globalbp/globalbp_uk_english/reports_and_publications/statistical_energy_review_2011/STAGING/local_assets/pdf/statistical_review_of_world_energy_full_report_2011.pdf (accessed June 1, 2012).

BP Energy. 2012. Statistical review of world energy. http://www.bp.com/assets/bp_internet/globalbp/globalbp_uk_english/reports_and_publications/statistical_energy_review_2011/STAGING/local_assets/pdf/statistical_review_of_world_energy_full_report_2012.pdf (accessed June 1, 2012).

Brichet, N., Weatherill, B., and Casale, E. 2002. The new ventilation systems of the Mont Blanc tunnel active smoke control: From simulation to successful operation. In *Proceedings of the 4th International Conference on Tunnel Fires*, Basel, Switzerland, pp. 95–113.

Broad, W. J. 2010. Iran shielding its nuclear efforts in maze of tunnels. http://www.nytimes.com/2010/01/06/world/middleeast/06sanctions.html?pagewanted=all&_r=0 (accessed May 24, 2012).

California Department of Industrial Relations (DIR). 2012. Tunnel safety orders. http://www.dir.ca.gov/title8/sb20a24apb.html (accessed September 29, 2012).

CargoCap. 2012. The CargoCap system. http://www.cargocap.com/content/the-cargocap-system (accessed July 12, 2012).

Carvel, R. 2008. Design fires for tunnel water mist suppression systems. In *International Symposium on Tunnel Safety and Security*, Stockholm, Sweden. http://www.tunnelfiresafety.co.uk/ (accessed July 4, 2012).

Carvel, R., Rein, G., and Torrero, J. 2009. Ventilation and suppression systems in road tunnels: Some issues regarding their appropriate use in a fire emergency. In *Second International Tunnel Safety Forum for Road and Rail*, Lyon, France, pp. 375–382. http://www.tunnelfiresafety.co.uk/ (accessed July 4, 2012).

Cordesman, A. 1999. *Iran's Military Forces in Transition*. Westport, CT: Praeger.

David, C. 1997. *Power at Odds: The 1922 National Railroad Shopmen's Strike*. Urbana, IL: University of Illinois Press.

De Decker, K. 2008. A world without trucks: Underground freight networks. http://www.lowtechmagazine.com/2008/02/a-world-without.html#more (accessed November 17, 2012).

Demetriou, D. 2012. North Korea building tunnel for third nuclear test. http://www.telegraph.co.uk/news/worldnews/asia/northkorea/9193861/North-Korea-building-tunnel-for-third-nuclear-test.html (accessed June 5, 2012).

Dongjun, G., Mingjian, Y., and Zhilong, C. 2007. A new choice for Shanghai container distribution—Underground container transportation system. In *11th ACCU Conference: Underground Space: Expanding the Frontiers*, Athens, Greece. http://www.minetech.metal.ntua.gr/extras/acuus2007/papers/section_04/ACUUS_093a.pdf (accessed November 17, 2012).

Earthquake Engineering Research Institute. 1990. Loma Prieta earthquake of January 17, 1994, Reconnaissance Report, *Earthquake Spectra*, Supplement to vol. 6.

Eastern Roads. 2012. Ted Williams Tunnel—Historic overview. http://www.bostonroads.com/crossings/ted-williams/ (accessed October 12, 2012).

EuDaly, K., Schafer, M., Boyd, J., Jessup, S., McBridge, A., and Glischinksi, S. 2009. *The Complete Book of North American Railroading*, pp. 1–352. Minneapolis, MN: Voyageur Press.

Gabbay, T. 2011. Bering Strait Tunnel to connect US and Russia? http://www.theblaze.com/stories/bering-strait-tunnel-to-connect-u-s-and-russia/ (accessed October 1, 2012).

Gedalyahu, T. B. 2010. Underground tunnels link Iran, Lebanon Gaza. http://www.israelnationalnews.com/News/News.aspx/135408#.UMfSqXfuB8E (accessed April 23, 2012).

Goff, Z., Patil, S., and Shih, C. 2000. Feasibility of freight pipelines to relieve highway congestions, Texas Department of Transportation and the US Department of transportation, Federal Highway Administration Funded Research. http://d2dtl5nnlpfr0r.cloudfront.net/tti.tamu.edu/documents/1803–1.pdf (accessed November 12, 2012).

Goodland, R. 2005. Oil and gas pipelines: Social and environmental impact assessment: State of the art. http://www.goodlandrobert.com/PipelinesBK.pdf (accessed December 1, 2012).

Haines, H. S. 1919. *Efficient Railway Operation*. Norwood, MA: The Macmillan Company.

He, C., Teng, L., and Yan, J. Y. 2008. *Geotechnical Aspects of Underwater Construction in Soft Ground*. Boca Raton, FL: CRC Press.

Helman, C. 2010. The World's Biggest Oil Reserves. http://www.forbes.com/2010/01/21/biggest-oil-fields-business-energy-oil-fields.html (accessed June 23, 2012).

History. 2012. Cu Chi tunnels. http://www.history.com/topics/cu-chi-tunnels (accessed September 29, 2012).

Hopkins, P. 2007. Oil and gas pipelines and today. http://www.penspen.com/Downloads/Papers/Documents/OilandGasPipelines.pdf (accessed December 1, 2012).

Hsu, J. 2009. Three extreme high-speed rail concepts for Las Vegas. http://www.popsci.com/technology/article/2009–10/three-extreme-high-speed-rail-systems-las-vegas (accessed November 17, 2012).

The Indian Express. 2012. Pak aped secret tunnel concept from North Korea: Indian Army. http://www.indianexpress.com/videos/national/6/pak-aped-secret-tunnel-concept from-n-korea-indian-army/11281 (accessed August 4, 2012).

International Atomic Energy Agency (IAEA). 2005. Regulations for the safety transport of radioactive material. http://www-pub.iaea.org/mtcd/publications/pdf/pub1225_web.pdf (accessed July 1, 2012).

International Atomic Energy Agency (IAEA). 2006. Safe transport of radioactive material. http://www-pub.iaea.org/MTCD/publications/PDF/TCS-01_4th_web.pdf (accessed July 4, 2012).

International Atomic Energy Agency (IAEA). 2008. Security in the transport of radioactive material. http://www-pub.iaea.org/MTCD/publications/PDF/pub1348_web.pdf (accessed July 4, 2012).

Iran Maglev Technology (IMT). 2012. Maglev magnetic levitation. http://www.maglev.ir/eng/education.html (accessed November 3, 2012).

Iran Nuclear. 2005. Iran's secret tunnel project to conceal its nuclear programs. http://irannuclear.org/index.php?option=com_content&task=view&id=32&Itemid=29 (accessed April 2, 2012).

Israel Ministry of Foreign Affairs. 2012. Operation pillar of defense—IDF updates. http://www.mfa.gov.il/MFA/Terrorism-+Obstacle+to+Peace/Terrorism+and+Islamic+Fundamentalism-/Operation_Pillar_of_Defense_Nov_2012-IDF_updates.htm?WBCMODE = PrCabinet_21-Mar-2010?DisplayMode=print (accessed December 10, 2012).

Jvarsheishivili, A. 1981. Pneumo-capsule pipelines in USSR, *J. Pipelines* 1(1):109–110.

Kosugi, S. 1992. A capsule pipelines in Japan and future developments. In *Proceedings of the International Symposium on Underground Transportation of Freight by Capsule Pipelines and Other Tube/Tunnel Systems*, Columbia, MO.

Licht, W. 1987. *Working for the Railroad: The Organization of Work in the Nineteenth Century*. Princeton, NJ: Princeton University Press.

Liu, H. 2000. Pneumatic capsule pipeline—Basic concepts, practical considerations, and current research. In *Proceedings of the 2000 Mid Continent Transportation Symposium*, Ames, IA. http://www.ctre.iastate.edu/pubs/midcon/liu.pdf (accessed November 17, 2012).

Long, Y. L. 2011. A second mega-TBM river crossing for Nanjing. http://www.tunneltalk.com/TBM-Recorder-Aug11-Mega-TBM-for-second-river-crossing-in-Nanjing.php (accessed September 24, 2011).

Malewitz, J. 2012. Unregulated pipelines raise safety concerns. http://www.pewstates.org/projects/stateline/headlines/unregulated-pipelines-raise-safety-concerns-85899378760 (accessed November 2012).

McDonald, C. 1993. The Federal Railroad Safety Program, US Federal Railroad Administration. http://www.fra.dot.gov/downloads/safety/rail_safety_program_booklet_v2.pdf (accessed November 27, 2012).

McGraw-Hill. 2012. Access science encyclopedia article. http://www.accessscience.com/abstract.aspx?id=100000&referURL = http%3a%2f%2fwww.accessscience.com%2fcontent.aspx%3fid%3d100000 (accessed August 20, 2012).

McPherson, G. and Laramore, R. 1990. *An Introduction to Electrical Machines and Transformers*, 2nd edn. New York: John Wiley & Sons.

National Aeronautics and Space Administration (NASA). 2012. Magnetic levitation space propulsion. http://www.maglev.ir/eng/documents/reports/IMT_R_9.pdf (accessed November 18, 2012).

National Fire Protection Association (NFPA). 2012a. Standard on selection, care, use, and maintenance of flame-resistant garments for protection of industrial personnel against flash fire, NFPA 2113.

National Fire Protection Association (NFPA). 2012b. All about fire. http://www.nfpa.org/itemDetail.asp?categoryID = 1330&itemID = 30861&URL = Press%20Room/A%20Reporter%27s%20Guide%20to%20Fire%20and%20the%20NFPA/All%20about%20fire (accessed July 4, 2012).

National Transportation Safety Board. 2011. Natural gas transmission pipeline rupture and fire, San Bruno, California, Pipeline Accident Report NTSB/PAR-11/01. http://www.ntsb.gov/doclib/reports/2011/PAR1101.pdf (accessed December 1, 2012).

National Wildfire Coordinating Group (NWCG). 2011. Glossary of wildland fire terminology. http://www.nwcg.gov/pms/pubs/glossary/pms205.pdf (accessed June 3, 2012).

Office of Safety and Health Administration (OSHA). 1996. Construction Safety and Health Outreach Program—Glossary of terms. http://www.osha.gov/doc/outreachtraining/htmlfiles/hazglos.html#tlv (accessed November 2, 2012).

Organization of the Petroleum Exporting Countries (OPEC). 2011. World oil outlook. http://www.opec.org/opec_web/static_files_project/media/downloads/publications/WOO_2011.pdf (accessed March 23, 2012).

Pakistan Defence. 2012. Tunnel found near India–Pak border. http://www.defence.pk/forums/indian-defence/198718-tunnel-found-near-india-pak-border.html (accessed December 1, 2012).

Parfomak, P. 2004. Pipeline security: An overview of federal activities and current policy issues. http://www.fas.org/sgp/crs/RL31990.pdf (accessed July 5, 2012).

PBS Press. 2012. Guerrilla tactics: An overview. http://www.pbs.org/battlefieldvietnam/guerrilla/index.html (accessed September 29, 2012).

People Daily 2002. China's First Double-Tube-and-Deck Cross-River Tunnel Completed in Shanghai. http://english.peopledaily.com.cn/200211/01/eng20021101_106106.shtml (accessed November 11, 2012).

Pipeline 101. 2007. Natural gas pipeline. http://www.pipeline101.com/Overview/natgas-pl.html (accessed June 23, 2012).

Powell, J. and Danby, G. 2005. Maglev: The new mode of transport for the 21st century. *21st Century Science and Technology Magazine*. http://www.21stcenturysciencetech.com/articles/Summer03/maglev2.html (accessed November 18, 2012).

Presutti, C. 2011. Scientists dispute university study in china's nuclear arsenal. http://www.voanews.com/content/scientists-dispute-university-study-on-chinas-nuclear-arsenal-135140753/168262.html (accessed June 4, 2012).

Purdue University. 2012. Pneumatic capsule pipeline. http://rebar.ecn.purdue.edu/ect/links/technologies/other/pcp.aspx (accessed November 17, 2012).

Queensland Government. 2012. Cross River Rail moving ahead as part of the Brisbane Inner Rail solution. http://www.crossriverrail.qld.gov.au/ (accessed December 9, 2012).

Ricci, T. 2012. Connecting two continents: The ultimate engineering challenge, American Society of Mechanical Engineers. http://www.asme.org/kb/news-articles/articles/arctic-engineering-offshore-technology/connecting-two-continents-the-ultimate-engineerin (accessed June 2, 2012).

Rodrigue, J. P. and Slack, B. 2012. Rail transportation and pipelines. http://people.hofstra.edu/geotrans/eng/ch3en/conc3en/ch3c3en.html (accessed November 25, 2012).

Roop, S., Olson, L., Warner, J., Morgan, C., Bierling, D., Roco, C., Kneepkens, R. et al. 2001. The technical and economic feasibility of a freight pipeline system in Texas—Year 2 report, Texas Department of Transportation and the US Department of Transportation, Federal Highway Administration Funded Research. http://d2dtl5nnlpfr0r.cloudfront.net/tti.tamu.edu/documents/1519–2.pdf (accessed November 12, 2012).

Roop, S., Olson, L., Warner, J., Morgan, C., and Rediniotis, O. 2000. The technical and economic feasibility of a freight pipeline system in Texas—Year 1 report, Texas Department of Transportation and the US Department of Transportation, Federal Highway Administration Funded Research. http://d2dtl5nnlpfr0r.cloudfront.net/tti.tamu.edu/documents/1519–1.pdf (accessed November 12, 2012).

Rothberg, P. 2005. Security threat assessments for HAZMAT drivers. http://www.fas.org/sgp/crs/RL32740.pdf (accessed August 3, 2007).

Russian International Affairs Council (RIAC). 2012. Tunnel construction under the Bering Strait: A new super goal for the Russian policy in APR? http://russiancouncil.ru/en/inner/?id_4=156 (accessed September 25, 2012).

Sandberg, H. and Williams, J. 2010. Design criteria for Maglev structures. *Iran Maglev Technol. J. Pap*., JP 60, Tehran, Iran. http://www.maglev.ir/eng/documents/papers/journals/IMT_JP_60.pdf (accessed November 18, 2012).

Schoesser, B. and Stein, D. 2003. CargoCap-transportation of goods through underground pipelines: Research project in Germany. In *Proceedings of the American Society of Civil Engineers (ASCE) International Conference on Pipeline Engineering and Construction*, Vol. 2, Baltimore, MD, July 2003. http://ascelibrary.org/doi/abs/10.1061/40690%282003%29181 (accessed July 12, 2012).

Shibata, S. and Murayama, S. 1995. Magnetic levitation transport system with non-contact inductive power supply and battery charging, US Patent, Patent No. 5,467,718, Osaka, Japan. http://www.google.com/patents?id=jwofAAAAEBAJ&printsec=abstract&zoom=4#v=onepage&q&f=false (accessed November 18, 2012).

Squires, G. Ed. 2002. Urban Sprawl: Causes, Consequences, & Policy Responses.: The Urban Institute Press. Washington D.C.

Stein, D. 2006. The use of pipelines and tunnels for the solution of future transport problems. http://www.pipeline-conference.com/sites/default/files/papers/4%20Stein.pdf (accessed November 20, 2012).

Technical Support Working Group. 2011. Pipeline Blast Mitigation Technologies. http://www.cttso.gov/publications/PBMTProjectReportSanitizedFINAL.pdf (accessed June 23, 2012).

The Telegraph. 2008. Chinese nuclear submarine base. http://www.telegraph.co.uk/news/worldnews/asia/china/1917167/Chinese-nuclear-submarine-base.html (accessed June 12, 2012).

Tomoji, F. 1994. Development of linear tube transportation system. *NKK Tech. J*. 70, 25–32.

Transit Cooperative Research Program (TCRP). 1997. Synthesis of transit practice 23: Inspection policy and procedures for rail transit tunnels and underground structures. http://onlinepubs.trb.org/onlinepubs/tcrp/tsyn23.pdf (accessed October 23, 2012).

Transit Cooperative Research Program (TCRP). 2003. Transit capacity and quality of service manual. http://www.trb.org/Main/Blurbs/153590.aspx (accessed October 3, 2012).

Transit Cooperative Research Program (TCRP). 2006. Transportation security: Making transportation tunnels safe and secure. http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v12.pdf (accessed November 29, 2012).

Trench, C. 2001. How pipelines make the oil market work—Their networks, operation, and regulation, A Memorandum Prepared for the Association of Oil Pipe Lines and the American Petroleum Institute's Pipeline Committee. http://pipeline101.org/reports/Notes.pdf (accessed November 12, 2012).

Tubular Rail Inc. (TRI). 2011. Rapid transit system—System evaluation. http://dot.cobbcountyga.gov/Rail_TUBULARRAILWHITEPAPER51211.pdf (accessed November 12, 2012).

Tubular Rail Inc. (TRI) 2012. Evolution of tubular rail. http://www.tubularrail.com/questions_answers.htm (accessed November 12, 2012)

United Press International (UPI). 2011a. Can Egypt secure its gas pipelines? http://www.upi.com/Business_News/Energy-Resources/2011/11/29/Can-Egypt-secure-its-gas-pipelines/UPI-76071322567666/ (accessed June 20, 2012).

United Press International (UPI). 2011b. Gas pipeline from Egypt bomb. http://www.upi.com/Business_News/Energy-Resources/2011/11/28/Gas-pipeline-from-Egypt-bombed/UPI-96601322489343/?rel=76071322567666 (accessed June 20, 2012).

United Press International (UPI). 2012a. Gas pipeline in Yemen attacked. http://www.upi.com/Business_News/Energy-Resources/2012/05/14/Gas-pipeline-in-Yemen-attacked/UPI-96171337000418/ (accessed June 20, 2012).

United Press International (UPI). 2012b. Terrorists attack Syrian gas pipeline. http://www.upi.com/Business_News/Energy-Resources/2012/01/03/Terrorists-attack-Syrian-gas-pipeline/UPI-26841325598451/ (accessed June 20, 2012).

US Bureau of Land Management (BLM). 2012. Mining claim information. http://www.blm.gov/az/st/en/prog/mining/requirements.html (accessed September 29, 2012).

US Department of Energy (DOE). 1999. Transporting radioactive materials. http://www.em.doe.gov/PDFs/transPDFs/ramquestions.pdf (accessed October 3, 2005).

US Department of Homeland Security (DHS). 2007. Transportation systems: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, Washington, DC.

US Department of Transportation (DOT). 2003a. Hazardous Material Transportation Safety and Security Field Operational Test Final Evaluation Plan. http://ntl.bts.gov/lib/jpodocs/repts_te/13844_files/13844.pdf (accessed May 20, 2005).

US Department of Transportation (DOT). 2003b. The role of hazardous material placards in transportation safety and security. http://www.phmsa.dot.gov/staticfiles/PHMSA/DownloadableFiles/Files/0803RedactedPlacardingReportSSI.pdf (accessed May 20, 2005).

US Department of Transportation (DOT). 2004a. HAZMAT safety and security field operational test. http://www.fmcsa.dot.gov/documents/hazmat/fot/hmfot-final-report.pdf (accessed June 3, 2012).

US Department of Transportation (DOT). 2004b. Hazardous materials safety and security technology field operational test—Volume II, Evaluation Final Report Synthesis. http://ntl.bts.gov/lib/29000/29500/29509/FINAL_Volume_II_HAZMAT_Synthesis__11–17–04.pdf (accessed June 3, 2012).

US Department of Transportation/Bureau of Transportation (DOT/BOT). 2002. Transportation indicators. http://www.bts.gov/publications/transportation_indicators/december_2002/entirepdf.pdf (accessed July 1, 2012).

US Department of Transportation/Federal Highway Administration (DOT-FHA). 2004. FHWA road tunnel design guidelines, Report No. FHWA-IF-05–023. http://ntl.bts.gov/lib/30000/30800/30876/FHWA-IF-05–023.pdf (accessed September 23, 2012).

US Department of Transportation/Federal Highway Administration. 2005. Highway and rail transit tunnel inspection manual. http://www.fhwa.dot.gov/bridge/tunnel/inspectman.pdf (accessed November 10, 2012).

US Department of Transportation/Federal Highway Administration. 2009. Technical manual for design of road tunnels—Civil elements. http://www.fhwa.dot.gov/bridge/tunnel/pubs/nhi09010/index.cfm (accessed November 1, 2012).

US Department of Transportation/Pipeline and Hazardous Materials Safety Administration (DOT-PHMSA). 2013. Gathering pipelines: What are the concerns in regard to unregulated gathering lines? (accessed January 22, 2013).

US Energy Information Administration (EIA). 2001. US natural gas markets: Recent trends and prospects for the future. http://www.eia.gov/oiaf/servicerpt/naturalgas/chapter_2.html (accessed June 12, 2012).

US Government Accountability Office (GAO). 2012. Pipeline safety: Collecting data and sharing information on federally unregulated gathering pipelines could help enhance safety. http://www.gao.gov/assets/590/589514.pdf (accessed August 23, 2012).

US Transportation Security Administration (TSA). 2012. Pipeline security. http://www.tsa.gov/what_we_do/tsnm/pipelines/index.shtm (accessed July 14, 2012).

Whaley, M. 2012. High-flying Ideas for I-70 Mountain Corridor in Colorado include "Tube Rail." http://www.denverpost.com/news/ci_21406822/high-flying-ideas-i-70-mountain-corridor-include (accessed November17, 2012).

Whatcom County Planning (WCP). 2001. Natural gas and hazardous liquid pipelines background report. http://www.mrsc.org/govdocs/w47pipelinerpt.pdf (accessed June 23, 2012).

World Nuclear Association (WNA). 2011. Transport of radioactive materials. http://www.world-nuclear.org/info/inf20.html (accessed July 13, 2012).

World Road Association/Permanent International Association of Road Congress (WRA-PIARC). 2011. Road tunnels manual. http://tunnels.piarc.org/en/ (accessed December 3, 2012).

Yaghoubi, H. 2011. The most important advantages of magnetically levitated trains. In *11th International Conference of Chinese Transportation Professionals (ICCTP)*, Nanjing, China. http://dx.doi.org/10.1061/41186(421)398 (accessed June 3, 2012).

Yaghoubi, H. 2012. Practical applications of magnetic levitation technology, Iran Maglev Technology, Final Report, Tehran, Iran. http://www.maglev.ir/eng/documents/reports/IMT_R_22.pdf (accessed June 3, 2012).

Yale University (YU). 2012. Flammable liquids. http://learn.caim.yale.edu/chemsafe/references/flammable.html (accessed March 2, 2012).

Zhang, C. and Wang, S. 2011. Comprehensive evaluation based on AHP-fuzzy about the conception of underground container transportation lines in Shanghai. *App. Mech. Mater. J*. 71–78, 175–181. Zurich, Switzerland: Trans Tech Publications. http://www.scientific.net/AMM.71–78.175 (accessed November 17, 2012).

Zhao, Y. and Lundgren, T. 2002. Characteristics of a freight pipeline transportation system. http://faculty.washington.edu/jbs/itrans/zhao.htm (accessed November 17, 2012).

Chapter 4

Risk and Vulnerability Assessment

4.1 Introduction

This chapter introduces the risk and vulnerability assessment for critical infrastructure protection, which can be utilized for pipelines, tunnels, rails, and transit systems mostly used and recommended by experts, the National Aeronautics and Space Administration (NASA), the US Department of Homeland Security (DHS), the Department of Transportation (DOT), the US National Counter Terrorism Center (NCTC), the Department of Defense (DoD), the National Commission on Terrorism (NCT), and other government agencies. Examples and applications of these standard processes and models will be presented in this chapter.

4.2 National Aeronautics and Space Administration Risk Analysis and Management

According to NASA (2011), in order to foster proactive risk management (RM), two complementary processes should be integrated: risk-informed decision making (RIDM) and continuous risk management (CRM); $RM = RIDM + CRM$. The RIDM process addresses the risk-informed selection of decision alternatives to assure effective approaches to achieve objectives, and the CRM process

addresses implementation of the selected alternative to assure that requirements are met (NASA 2011). As applied to CRM, risk is characterized as a set of triplets (NASA 2011):

- The *scenario(s)* leading to degraded performance with respect to one or more performance measures (e.g., scenarios leading to injury, fatality, destruction of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage).
- The *likelihood(s)* (qualitative or quantitative) of those scenarios.
- The *consequence(s)* (qualitative or quantitative severity of the performance degradation) that would result if those scenarios were to occur.

RIDM is invoked for key decisions such as architecture and design decisions, make-buy decisions, source selection in major procurements, and budget reallocation (allocation of reserves), which typically involve requirements-setting or rebaseling of requirements (NASA 2011). In the *Risk Analysis of Alternatives*, the performance measures of each alternative are quantified, taking into account any significant uncertainties that stand between the selection of the alternative and the accomplishment of the objectives (NASA 2011). Hence, the estimates of expected consequences alone do not adequately inform technical decisions (NASA 2007a). Based on the *NASA Systems Engineering Handbook* (NASA 2007a), *scenario-based analyses* provide more of the information that risk-informed decisions need; for instance, a rare but severe risk contributor may warrant a response different from the one warranted by a frequent, less severe contributor, even though both have the same expected consequences. The *risk analysis of decision alternatives* not only guides the selection of a preferred alternative, but it also carries out the "identify" and "analyze" steps of CRM (NASA 2007a). NASA utilized the following quantitative methods.

4.2.1 Risk Matrices

The "N × M" risk matrices provide assistance in managing and communicating risk and help to (a) track the status and effects of risk-handling efforts and (b) communicate risk status information (NASA 2007a). Different organizations, and sometimes projects, establish their own format and a definition widely used by NASA, other government organizations, and industry is provided (NASA 2007a):

- *Low (light gray) risk*: Has little or no potential for increases in cost, disruption of schedule, or degradation of performances
- *Moderate (dark gray) risk*: May cause some increase in cost, disruption of schedule, or degradation of performance
- *High (black) risk*: Likely to cause significant increase in cost, disruption of schedule, or degradation of performance (Figure 4.1)

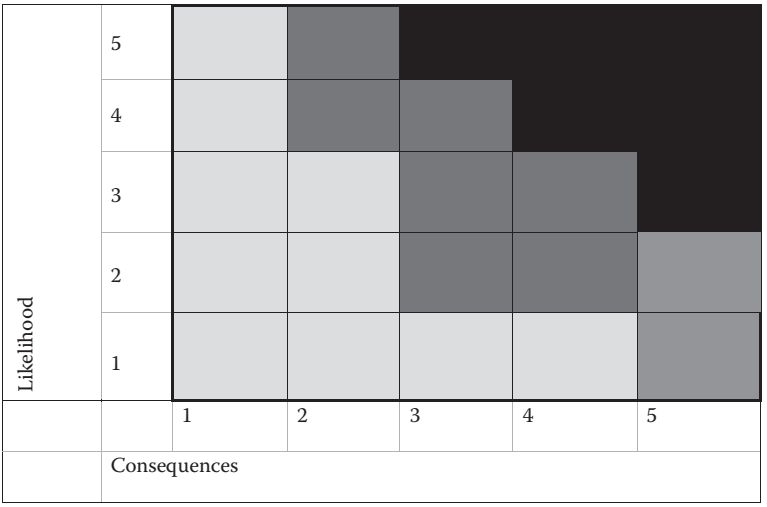


Figure 4.1 N×M risk matrices. (From National Aeronautics and Space Administration, *NASA System Engineering Manual*, 2007a. http://www.acq.osd.mil/se/docs/NASA-SP-2007–6105-Rev-1-Final-31Dec2007.pdf, accessed on February 23, 2013.)

4.2.2 FMECAs, FMEAs, and Fault Trees

Failure modes, effects, and criticality analysis (FMECA), failure modes and effects analysis (FMEA), and fault trees are methodologies designed to identify potential failure modes for a product or process, to assess the risk associated with those failure modes, to rank the issues in terms of importance, and to identify and carry out corrective actions to address the most serious concerns (NASA 2007a).

4.2.3 NASA Probabilistic Risk Assessment

A probabilistic risk assessment (PRA) is applied to identify and evaluate risks affecting safety and health (i.e., having a potential for injury or illness, loss of life, damage, or unexpected loss of equipment, as well as those affecting the ability to reliably meet mission objectives) (NASA 2010). A PRA characterizes risk in terms of three basic questions: (1) *What can go wrong?* (2) *How likely is it?* (3) *What are the consequences?* (NASA 2010). The process of conducting a PRA is (NASA 2010) as follows:

- *Step 1:* Definition of objectives
- *Step 2:* Scenarios development
- *Step 3:* Quantification and uncertainty analysis
- *Step 4:* Interpretation of results
- *Step 5:* Documentation

The purpose of a PRA is to provide risk information for decision making during various phases of a program/project life cycle (NASA 2010). Risk information is used as an input for decisions involving concept, architecture and mission formulation, functional and hardware design after including humans and software, and mission operations.

4.3 Standard Homeland Security Risk Assessment and RAMCAP Plus Processes

It is widely recommended by experts and government agencies and is employed in conjunction with other vulnerability assessment processes such as Risk Analysis and Management for Critical Asset Protection *(RAMCAP Plus)*. In this method, *resilience* is the majority determination but not part of the risk calculations. Resilience is defined as the ability to operate and survive from man-made disaster in which an asset can return to its full function.

Risk is the estimated loss from a future sequence of events with an undesirable negative outcome. The total system risk (R) is the summation of the risks from all possible events. The events arising from one or many threats and initiating actions may lead to different risk scenarios, which in turn have many possible outcomes. In the standard risk assessment methodology, the *risk* (R) assessment formula is as follows: *threat* (T) to a target/area multiplied by *vulnerability* (V) of the target/area multiplied by *consequence* (C) of an attack on that target/area or

$$R = T \times V \times C \tag{4.1}$$

For the asset owner, the level of resilience for a particular threat is expressed as (ASME-ITI 2009)

$$\text{Resilience}_{(\text{owner})} = \text{Lost revenue} \times \text{Vulnerability} \times \text{Threat} \tag{4.2a}$$

For the community, the level of resilience for a particular threat is expressed as

$$\text{Resilience}_{(\text{community})} = \text{Lost economic activity in the community} \times \text{Vulnerability} \times \text{Threat} \tag{4.2b}$$

The lost revenue is the product of the duration of service (in days), the extent of service denial (in units of service denied per day), and the price per unit (in dollars, estimated at pre-event levels), which are all essential parts of estimating the owner's financial loss:

$$\text{Loss revenue} = \text{Duration of denial} \times \text{Severity of denial} \times \text{Price per unit} \quad (4.2c)$$

The loss of economic activity in the society is the reduction balance in the loss of output to direct customers and the indirect losses (multiplier effect) throughout the economy of a given region due to denial of service. An example is provided below. There are seven ways used in the risk estimation:

1. Asset classification
2. Threat definition
3. Consequence analysis
4. Vulnerability analysis
5. Threat evaluation
6. Risk analysis
7. Value of consequence

These seven steps of risk estimation for terrorist attacks and disasters are shown in Tables 4.1 through 4.12.

Consequence scales for fatalities, injuries, financial losses to owners or operators, and economic losses to the society are developed based on the RAMCAP Plus process for oil and gas pipelines, tunnels, underground rail, and transit systems. There are several methods for quantifying the consequence scale for specific sectors, events, and situations or conditions for a specific area and area boundaries based on the political, environmental, and economic status of the subject area. The consequence scale can be determined according to statistical data.

Quantitative estimation or an engineer's discretion for estimation can be done when the subject area lacks statistical information. Aerial photographic maps, topographic/site surveys, or geographic information system (GIS) and statistical data provided by the federal/local government or by the commercial industry can be utilized to analyze and gain information of specific damage, fatalities, injuries, people, equipment, and materials. In Tables 4.4 through 4.6, the range of each bin increases by a factor of two over the next bin. The scaling factor provides a logarithmic scale for scientific presentation purposes, in this case one at base 2.

The vulnerability scale presented in Table 4.10 uses a scale factor of 2, enabling construction of a conditional risk table of consequence and vulnerability scales with the sum of their "bin numbers" being the logarithm of the conditional risk (ASME-ITI 2009). The bin numbers and vulnerability scale values are applicable for pipelines, tunnels, capsule freight transportation, underground rail, and transit systems based on the RAMCAP Plus process and DHS methods. This will produce a convenient, qualitative display of results as the conditional risk matrix will contain diagonal lines of constant risk.

Table 4.1 Step 1: Asset Characterization for Pipelines, Tunnels, Rail, and Transit Systems

1. Oil and gas pipelines and their facilities: a. Primary energy source b. Transport of flammable and hazardous material c. Can generate public hazard when the materials are exposed to the environment d. Gathering and trunk lines including storage tanks are not secured
2. Aqueducts (water pipelines): a. "Lifeblood" of Southern California, Los Angeles, and Hollywood (one of the primary economic mechanisms in the United States) b. Main water source of New York City c. Basic security systems
3. Railroad/railway system: a. Transportation of hazardous and radioactive materials b. Major use for hauling operations in urban and interurban areas c. Unsecured
4. Immersed tunnel or underwater tunnel: a. Major rail network and transportation system b. To connect to large metropolitan areas for trade and industry c. Unsecured
5. Road and highway tunnels: a. Located at key choke points in the transportation network b. Move thousands of people and cargo regularly c. Unsecured
6. Underground high-speed rail transportation system (magnetic levitation or maglev): a. Provide mobility in over populated areas during all peak hours b. Provide fast manpower mobilization c. Futuristic advanced transportation technology d. Greatly improved productivity of freight services e. Unsecured

Table 4.1 (continued) Step 1: Asset Characterization for Pipelines, Tunnels, Rail, and Transit Systems

7. Tubular rails: a. Provide mobility in overpopulated areas during all peak hours b. Provide fast manpower mobilization c. Futuristic advanced transportation technology d. Greatly improved productivity of freight services e. Unsecured
8. Underground freight capsule pipelines and CargoCap: a. Efficiently provide fast cargo/freight transshipment and economic growth b. Provide a significant decrease of transport time and environment-friendly

Table 4.2 Step 2: Threat Characterization for Pipelines, Tunnels, Rail, and Transit Systems

1. Placing of improvised explosive devices
2. Suicide bombers
3. Sabotage pipelines
4. Placing of weapons of mass destruction (WMD) in maglev and tubular rails
5. Ignition of flammable material to freight system
6. Generate electromechanical failure and/or cyber-controller system failure
7. Generate rail derailment and collision
8. Underground trains can be used for illegal secret transshipment of WMD and smuggling of manpower for WMD production
9. Generate floods into tunnels

4.3.1 Fatalities and Serious Injuries

In RAMCAP Plus, human health and safety consequences should be conveyed in terms of the number of *fatalities* and *serious injuries* that occur immediately as a result of disaster events (e.g., lost work time and disability).

4.3.2 Financial and Economic Impacts

Usually, economic and financial impacts are measurements of consequences in analyzing risks from man-made and natural disasters. The owners and operators of the

Table 4.3 Step 3: Consequence Analysis for Pipelines, Tunnels, Rail, and Transit

1. Financial and economic impacts: a. Replacement costs b. Business interruption c. Negative impact on other sectors d. Loss of business dependent on oil and gas supplies e. Disrupt downstream commercial, agriculture, and industry infrastructure due to aqueduct destruction f. Collapse of key transportation and freight systems network (infrastructures) g. Result in economic distress due to the tremendous need for reconstruction of infrastructures
2. Human health injury
3. Environmental impact: a. Injure endangered species b. Damage other key resources c. Radiation poisoning
4. Psychological impacts: a. Damage public confidence and morale
5. Loss of aqueducts and underground transshipment network
6. Regional/national security functionality impacts

water infrastructure are responsible for maintaining the security of their facilities, reliability of their services, and financially sustainable operations. The general public served by the facility is normally represented by public authorities and public/private partnerships. As indicated by ASME-ITI (2009), in the RAMCAP Plus process, when quantifying the owner's losses, the principle is that value, whether gain or loss is the incremental discounted net present value of future cash flows. The elements of the owner's loss include but are not limited to

1. Business interruption costs
2. Downstream industry interruption costs
3. Environmental remediation
4. Costs involved in repair of equipment/structures
5. Replacement costs
6. Reconstruction or rehabilitation costs
7. Liability costs and other costs contributed by the attack

Table 4.4 Consequence Scale for Fatalities

Number of Fatalities	*Consequence Scale—Fatalities*								
Consequence criteria ("bin numbers")	0	1	2	3	4	5	6	7	8
Ranges in number of fatalities	0–20	21–40	41–80	81–160	161–320	321–640	641–1,280	1,281–2,560	2,561–5,120
Consequence criteria ("bin numbers")	9	10	11	12	13	14	15	16	
Ranges in number of fatalities	5,121–10,240	10,241–20,480	20,481–40,960	40,961–81,920	81,921–163,840	163,841–327,682	327,681–655,360	655,361–+	

Sources: Derived from American Society of Mechanical Engineers Innovative Technologies Institute, LLC., *All-Hazards Risk and Resilience Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach*, ASME, New York, 2009; Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

Table 4.5 Consequence Scale for Injuries

Number of Injuries	*Consequence Scale—Injuries*								
Consequence criteria ("bin numbers")	0	1	2	3	4	5	6	7	8
Ranges in number of injuries	0–20	21–40	41–80	81–160	161–320	321–640	641–1,280	1,281–2,560	2,561–5,120
Consequence criteria ("bin numbers")	9	10	11	12	13	14	15	16	
Ranges in number of injuries	5,121–10,240	10,241–20,480	20,481–40,960	40,961–81,920	81,921–163,840	163,841–327,682	327,681–655,360	655,361–+	

Sources: Derived from American Society of Mechanical Engineers Innovative Technologies Institute, LLC., *All-Hazards Risk and Resilience Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach*, ASME, New York, 2009; Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

Table 4.6 Consequence Scale for Economic and Financial Impacts to the Owner/Operator

Financial Loss	*Consequence Scale—Financial Impacts to the Owner/Operator*								
Consequence criteria ("bin numbers")	0	1	2	3	4	5	6	7	8
Owner/operator financial loss ($1M)	0–20	21–40	41–80	81–160	161–320	321–640	641–1,280	1,281–2,560	2,561–5,120
Consequence criteria ("bin numbers")	9	10	11	12	13	14	15	16	
Owner/operator financial loss ($1M)	5,121–10,240	10,241–20,480	20,481–40,960	40,961–81,920	81,921–163,840	163,841–327,682	327,681–655,360	655,361–+	

Sources: Derived from American Society of Mechanical Engineers Innovative Technologies Institute, LLC., *All-Hazards Risk and Resilience Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach*, ASME, New York, 2009; Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

Table 4.7 Consequence Scale for Economic and Financial Impacts to the Regional Community

Number of Fatalities	*Consequence Scale—Economic/Financial Impacts ($1M)*								
Consequence criteria ("bin numbers")	0	1	2	3	4	5	6	7	8
Regional community economic loss ($1M)	0–20	21–40	41–80	81–160	161–320	321–640	641–1,280	1,281–2,560	2,561–5,120
Consequence criteria ("bin numbers")	9	10	11	12	13	14	15	16	
Regional community economic loss ($1M)	5,121–10,240	10,241–20,480	20,481–40,960	40,961–81,920	81,921–163,840	163,841–327,682	327,681–655,360	655,361–+	

Sources: Derived from American Society of Mechanical Engineers Innovative Technologies Institute, LLC., *All-Hazards Risk and Resilience Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach*, ASME, New York, 2009; Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

Table 4.8 Probable Consequences Based on the Threats against Pipelines, Tunnels, Rail, and Transit Systems

	Consequences	
Sabotage on rail and transit systems in one of the major (large) metropolitan areas	Bin number	Remarks
Fatalities	7	In communities near rail transportation system
	6	In overpopulated locations near rail and transit systems
	1–3	Passengers of rail and transit systems
Injuries	6	
Financial impact to owner/operator	3	Reconstruction of rail and transit network
	6–10	Overall total loss could go up higher
Regional community economic impact	6 or higher	Businesses/industry cannot operate due to disruption in transportation/transshipment network
Environmental, psychological, and ecological impacts	Not quantified	Not quantified in RAMCAP Plus
Blasting of oil and gas pipelines	Bin Number	Remarks
Fatalities	0–1	Blasting of several oil and gas pipelines (trunk lines and storage tanks)
Injuries	1	
Financial impacts to owner/operator	5	Repair cost and remediation cost
Regional community economic impact	5 or higher	Cost of remediation and recovery

(*continued*)

Table 4.8 (continued) Probable Consequences Based on the Threats against Pipelines, Tunnels, Rail, and Transit Systems

	Consequences	
Sabotage on aqueducts	Bin number	Remarks
Fatalities	0–1	Affluent communities
	5 or higher	Middle-class/lower middle-class communities (due to floods from aqueducts explosions)
	4	Rural areas
Injuries	4	Overall
Financial impact to owner/operator	10	Reconstruction of aqueducts
	6–10	Overall total loss could go up higher
Regional community economic impact	6 or higher	Remediation, recovery, and construction of advance treatment

Sources: Derived from American Society of Mechanical Engineers Innovative Technologies Institute, LLC., *All-Hazards Risk and Resilience Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach*, ASME, New York, 2009; Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

Table 4.9 Vulnerability Analysis for Pipelines, Tunnels, Rail, and Transit Systems

Vulnerability Analysis
1. Basic security implemented to aqueducts and mostly located in open spaces.
2. Oil and gas pipelines have deficiency in security—*gathering lines* are not protected and trunk lines have basic security that can certainly be sabotaged.
3. Underground high-speed (*maglev*) rail and transit systems are not secured and do not have high-standard preventive measures.
4. Tubular rail technology does not have high-standard preventive measures.
5. Immersed tunnel or underwater tunnel and cross-river tunnels do not have high-standard preventive measures.

Table 4.10 Vulnerability Scale

Bin (Category)		*Probabilities in Decimal Description*	*Probabilities in Percentage Description (%)*
5	a	0.85–1.00	85–100
	b	0.65–0.84	65–84
	c	0.40–0.64	40–64
4		0.20–0.398	20–39.8
3		0.10–0.198	10–19.8
2		0.05–0.099	5–9.9
1		0.025–0.049	2.5–4.9
0		<0.024	0–2.4

Sources: Derived from American Society of Mechanical Engineers Innovative Technologies Institute, LLC., *All-Hazards Risk and Resilience Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach*, ASME, New York, 2009; Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

In the public perspective of water infrastructure, the major concern is the length of time and quantity of service denied and the economic consequences of service denial on direct suppliers and customers of the critical facilities.

The economic loss can be as much as three orders of magnitude greater than the gross revenue losses of the facility. According to ASME-ITI (2009), in the RAMCAP Plus method, estimating the economic impacts of the community requires a regional simulator or an economic model to fully capture cascading failures and indirect/direct consequences and requires a system model that simulates pipelines, tunnels, underground rail, and transit systems. The conventional input–output models used in estimating the consequences of a major disruption or attack can lead to major errors. The economic losses shown in Table 4.3 are estimated by approximation using the RAMCAP Plus process. The regional economic loss estimate can serve as a baseline for the resilience of the region and it includes all the affected elements: the severity and time of service denial, economic consequences, and public health impact (due to emission of toxic substance, explosion of hazardous debris, and burst of missiles and fragments). Table 4.3 shows the consequences based on the threats shown in Table 4.2.

Table 4.11 Threat Assessment for Pipelines, Tunnels, Rail, and Transit Systems

Threat Assessment (Three Methods)
1. Numerical ratio method: *This estimate can be based on historical data, intelligence information, or various assumptions* a. Let T = number of attacks attempted on the United States b. Assuming the probability of attacking (some of the) pipelines, tunnels, rapid rail, and transit systems is equal to all other 18 sectors c. Probability (P) = T/18 for terrorist attacks d. Assuming based on the data, there are W facilities e. Let W = 30,000 system facilities; $P = (T/18)/30{,}000 \sim 0.00000185T$ f. Assuming the particular target being evaluated has eight major assets: $P = (T/18)(W \times 8)$ g. Let T = 8 attacks h. $P = (8/18)/(30{,}000 \times 8) = 1.85 \times 10^{-6}$ events/year
2. Comparison of risk tolerance with natural hazard risk uses the idea of risk tolerance and a natural hazard risk to compare with a terrorist risk to deduce a threat probability equating the two risks a. Consider the *standard Homeland Security* risk equation, $R = C \times V \times T$ b. Transpose to $T = R/(C \times V)$ c. Assume rapid transportation systems recovery/reconstruction cost = $5B d. Net cash flow after taxes = $10B e. Tornado risk = 150–250 mph (only an assumption) f. Assume tornado risk for the rapid transportation systems and some pipelines = $80M g. The total owner's loss of $3B after shutting down for 9 months and for reconstruction h. Vulnerability (V) = 0.75 (treatment plants with security system at entrance/exit) i. $T = (80{,}000{,}000)/(5{,}000{,}000{,}000 \times 0.75) = 0.0213$ events/year j. Frequency = 1/0.0213 = 47 years

Table 4.11 (continued) Threat Assessment for Pipelines, Tunnels, Rail, and Transit Systems

Threat Assessment (Three Methods)
3. Investment breakeven *assumes the decision maker's choices are simple on individual options* $R = T \times V \times C$, DHS standard risk equation/RAMCAP Plus equation Minimum benefits to justify the option's cost: (baseline risk – option risk [R])/$\text{Cost}_{\text{option}} > 1.0$ Therefore, $\{[(C_{\text{baseline}} \times V_{\text{baseline}}) - (C_{\text{option}} \times V_{\text{option}})] \times T\}/\text{Cost}_{\text{option}} = 1.0$ Continuing the example from (b), a series of countermeasures were delineated at a cost of \$80M The option was approximated to decrease vulnerability from 0.75 to 0.40 and reduce the consequence to the owner from \$2B to \$0.8B $C_{\text{baseline}} = \$2\text{B}$; $C_{\text{option}} = \$0.8\text{B}$ $T = \text{Cost}_{\text{option}}/\{[C_{\text{baseline}} \times V_{\text{baseline}}] - (C_{\text{option}} \times V_{\text{option}})\}$ $T = \$80\text{M}/\{(\$2\text{B} \times 0.75) - (\$0.8\text{B} \times 0.40)\}$ $T = \$50\text{M}/\$1.18\text{B} = 0.042$ or a reoccurrence of $1/0.042 = 23.8$ years

Source: Derived from American Society of Mechanical Engineers Innovative Technologies Institute, LLC., *All-Hazards Risk and Resilience Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach*, ASME, New York, 2009.

4.3.3 Vulnerability Analysis

Vulnerability analysis estimates the conditional likelihood that a threat will have the consequences estimated in Step 3. It estimates the probability that the terrorist will be successful in executing a specific attack. Table 4.9 presents Step 4 of RAMCAP Plus. The vulnerability scale is shown in Table 4.10, and the scale uses the same factor of 2 between successive categories, as in consequence ranking. This is effective for plotting a resultant risk matrix. Category 5 is further subdivided into three subcategories: a, b, and c. It is feasible for the owner/operator to estimate changes in security and defense level in RM.

4.3.4 Threat Assessment

Threat assessment determines the probability of each initiating negative event. In RAMCAP Plus, risk assessment for terrorism consists of weighing available evidence about an adversary and the asset in question. An example of threat assessment is presented in Table 4.11.

Table 4.12 Risk and Resilience Assessment for Tunnels, Rail, and Transit Systems

Threat Assessment		
1. Example from Step 3:		
Pipelines and railways terrorism (similar scenario—"Ufa train disaster" on June 1989 in the Soviet Union)	Bin number	Remarks
Fatalities	6	575 people died.
		Resulting from an explosion of a leaking natural gas line. Approximately 300 tons of TNT equivalent explosions. More than 97% people were burned.
Injuries	6	800 were injured.
Financial impacts to owner/operators	3	It is assumed that $2B will be required to reconstruct pipelines and rail system, environmental remediation, and insurance liability.
	6–10	Overall total loss could go up higher.
Regional community economic impacts	6 or higher	Business cannot operate due to severe contamination in the area if one rail system was carrying radioactive material.

Table 4.12 (continued) Risk and Resilience Assessment for Tunnels, Rail, and Transit Systems

Threat Assessment
2. Consequence are summarized as follows: Fatalities = 500 Acute injuries = 800 Financial impact to the owners = \$100B Losses to the regional economy = \$300B+ *Consequences of damages to the natural resources—environmental, psychological impact is not quantified in RAMCAP Plus*
3. Vulnerability: (Rail system is unprotected—no need of any expertise to intrude) 0.95
4. Threat: The probability of having an attack per Step 4 1.85×10^{-6} events/year
5. Risk: a. Fatalities: $R_f = 575 \times 0.95 \times (1.85 \times 10^{-6}) = 0.001$ lives/year b. Injuries: $R_i = 800 \times 0.95 \times (1.85 \times 10^{-6}) = 0.0014$ lives/year c. Financial impacts to the owner: $R_{O\$} = \$100B \times 0.95 \times (1.85 \times 10^{-6}) = \$175{,}800$ d. Economic losses to regional economy: $R_{\text{REGION}\$} = \$300B \times 0.95 \times (1.85 \times 10^{-6}) = \$527{,}400$

Sources: Derived from American Society of Mechanical Engineers Innovative Technologies Institute, LLC., *All-Hazards Risk and Resilience Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach*, ASME, New York, 2009; Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

4.3.5 Risk and Resilience Assessment

Risk and resilience assessment is the backbone for determining strategies for protection against sabotage and disaster by establishing priorities based on the level of risk. The risk imposed by each threat to each asset is calculated from the risk relationship: $R = T \times V \times C$. For the asset owner, the level of resilience for a particular threat is expressed as the product of lost revenue, vulnerability, and threat (Equation 4.2a). For the community, the level of resilience for a particular threat is

the product of lost economic activity in the community, vulnerability, and threat (Equation 4.2b). Lost revenue is the product of the duration of service denial, the extent of service denial, and the price per unit (Equation 4.2c). Lost economic activity in the community is the level of decrease in the loss of positive output to direct customers and the indirect losses throughout the entire economy of a given region or community due to denial of service and its extent.

4.3.6 Risk and Resilience Management

According to ASME-ITI (2009), in RAMCAP Plus, risk and resilience management is the deliberate course of deciding and implementing options (e.g., improving preventive measures, mitigation tactics, building in redundancy, creating emergency response plans, exercise business casualties) and achieving an acceptable level of risk and resilience at an acceptable cost to the organization and the community. Risk and resilience management based on RAMCAP Plus will not be presented in detail in this book.

4.4 Department of Defense Risk Assessment and Management

RM is the process by which decision makers are provided with the necessary information to accept, reduce, or offset risk (DoD 2013). As the DoD RM program, the Defense Critical Infrastructure Program (DCIP) seeks to ensure the availability of networked assets critical to DoD missions (DoD 2013). Risk assessment is a systematic examination of risk using disciplined processes, methods, and tools which provides an environment for decision making to continuously evaluate and prioritize risks and recommend strategies to remediate or mitigate those risks (DoD 2013). Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule, and performance constraints (DoD 2006). Risks have three components (DoD 2006):

- A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring; it is the most basic reason for the presence of a risk.
- A probability (or likelihood) assessed at the present time of that future root cause occurring.
- The consequence (or effect) of that future occurrence.

The fundamental risk assessment guidance for the DoD is the "Risk Management Guide for DoD Acquisition" (JITC 2013). Although the principles explained in the guide are not mandatory, they are recommended and applicable to DoD Information Technology Standard Registry (DISR) and non-DISR standards

(JITC 2013). By organizing the risk analysis, potential issues may be eliminated from consideration due to low mission impact and/or low probability of occurrence (likelihood of failure) (JITC 2013). The Department of the Air Force (DOAF 2003) stated that the seriousness of a risk can be determined by multiplying the probability of the event actually occurring by the potential negative impact to the cost, schedule, or performance of the project: *risk severity = probability of occurrence × potential negative impact*.

Traceability is a required management activity where requirements are traced back to their original higher-level requirement sources (DOAF 2003). This ensures that all higher-level requirements are being met by detailed requirements (DOAF 2003). Tailoring traceability based on risk maximizes benefit realization. As the risk of counterfeiting increases along with the consequence, more rigorous countermeasures must be taken throughout the supply chain (DoD 2012a).

4.4.1 Risk Reporting Matrix

The Risk Reporting Matrix is typically used to determine the level of risks identified with a program and the level of risk for each root cause is reported as low (light gray), moderate (dark gray), or high (black) (DoD 2006). The DoD Risk Assessment Guide recommends calculating risk according to the Risk Reporting Matrix shown in Figure 4.2, where the terms impact and consequence are synonymous (JITC 2013).

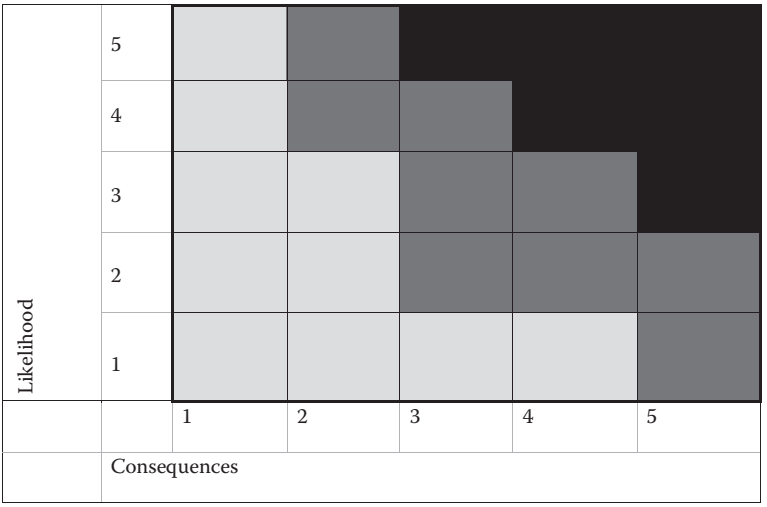


Figure 4.2 Risk reporting matrix. (From US Department of Defense, *Risk Management Guide for DOD Acquisition*, 6th edn., Department of Defense, Fort Belvoir, VA, 2006. http://www.acq.osd.mil/damir/documents/DAES_2006_RISK_GUIDE.pdf, accessed August 18, 2012.)

Table 4.13 Levels of Likelihood Criteria

Level	*Likelihood*	*Probability of Occurrence (%)*
1	Not likely	~10
2	Low likelihood	~30
3	Likely	~50
4	Highly likely	~70
5	Near certainty	~90

Source: US Department of Defense, *Risk Management Guide for DOD Acquisition*, 6th edn., Department of Defense, Fort Belvoir, VA, 2006. http://www.acq.osd.mil/damir/documents/DAES_2006_RISK_GUIDE.pdf (accessed August 18, 2012).

The level of likelihood of each root cause is established utilizing specified criteria as shown in Table 4.13 (DoD 2006).

Risk varies proportionally with likelihood (JITC 2013). The likelihood of each known issue should be estimated using another standard scale based on the derived risk assessment of JITC (2013) in Table 4.14.

The levels and types of consequences of each risk are established utilizing criteria such as those described in Table 4.15 (DoD 2006). Continuing with the prior example of a root cause with a 50% probability of occurring, if that same root cause

Table 4.14 Likelihood Levels

Level	*Likelihood*	*Probability of Occurrence Criteria (%)*
1	Not likely	0–20
2	Low likelihood	21–40
3	Likely	41–60
4	Highly likely	61–80
5	Near certainty	81–100

Source: Joint Interoperability Test Command, JITC risk assessment methodology, 2013. http://jitc.fhu.disa.mil/cgi/jsr/downloads/nrkpp_guidebook_appdxe.pdf (accessed April 17, 2013).

Table 4.15 Levels and Types of Consequence Criteria

Level	*Technical Performance*	*Schedule*	*Cost*
1	Minimal or no consequence to technical performance	Minimal or no impact	Minimal or no impact
2	Minor reduction in technical performance or supportability, can be tolerated with little or no impact on program	Able to meet key dates Slip < [a] month(s)	Budget increase or unit production cost increases < [b] (1% of budget)
3	Moderate reduction in technical performance or supportability with limited impact on program objectives	Minor schedule slip. Able to meet key milestones with no schedule float. Slip < [a] month(s) Subsystem slip > [a] month(s) plus available float	Budget increase or unit production cost increase < [b] (5% of budget)
4	Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success	Program critical path affected Slip < [a] month(s)	Budget increase or unit production cost increase < [b] (10% of budget)
5	Severs degradation in technical performance; cannot meet KPP or key technical/supportability threshold; will jeopardize program success	Cannot meet key program milestones Slip > [a] month(s)	Exceeds APB threshold > [b] (10% of budget)

Source: US Department of Defense, *Risk Management Guide for DOD Acquisition*, 6th edn., Department of Defense, Fort Belvoir, VA, 2006. http://www.acq.osd.mil/damir/documents/DAES_2006_RISK_GUIDE.pdf (accessed August 18, 2012).

[a] Number of months.
[b] Amount of cost.

Table 4.16 Impact Levels

Impact Level	*Technical Performance Criteria*
1	Minimal or no consequence to technical performance.
2	Minor reduction in technical performance. Can be tolerated with little or no impact on program.
3	Moderate reduction in technical performance. May jeopardize program success.
4	Significant degradation in technical performance. May jeopardize program success.
5	Severe degradation in technical performance. Cannot meet key technical threshold. Will jeopardize program success.

Source: Joint Interoperability Test Command., JITC risk assessment methodology, 2013. http://jitc.fhu.disa.mil/cgi/jsr/downloads/nrkpp_guidebook_appdxe.pdf (accessed April 17, 2013).

has no impact on performance or cost, but may likely result in a minor schedule slippage that won't impact a key milestone, then the corresponding consequence is a level 3 for this risk (DoD 2006).

Risk varies proportionally with impact and critically is an indication of impact, and the impact of each known issue should be estimated using a standard scale (JITC 2013) as provided in Table 4.16.

Likelihood and impact risk factors are independent of each other (i.e., a change in the likelihood of an error will not affect the impact to the operational mission if an error occurs (JITC 2013). Risk to the trust in applicable systems is managed throughout the entire life cycle of the system (DoD 2012b). The application of RM practices begins during the design of applicable systems and prior to the acquisition of critical components or their integration within applicable systems, whether acquired through a commodity purchase, system acquisition, or sustainment process (DoD 2012b).

4.4.2 Security Risk Categories

The DoD components use the Tables 4.17 through 4.21 for computation of security risk categories (SRC) to determine the numerical value of each risk factor (utility, casualty or damage, adaptability, and portability) and to compute the overall risk and SRC (DoD 2012c). To determine the numerical rating corresponding to risk, select one value from each table (Tables 4.17 through 4.20) and then total the four numbers (DoD 2012c). Use the total to obtain the overall SRC value from the risk factor SRC conversion table (Table 4.21).

Table 4.17 Utility Risk Factor Values

Utility	*Risk Factor*	*Description*
High	1	High-explosive, concussion, and fragmentation devices.
Moderate	2	Small arms ammunition.
Low	3	Ammunition items not described in section 4 (*uncategorized (CAT-U) Arms, Ammunition, and Explosives; AA&E and/or generally exceed an unpacked weight of 100 pounds shall have security policy developed by the responsible DoD component*) of this enclosure. Nonlethal munitions, civil disturbance chemicals, incendiary devices.
Impractical	4	Practice, inert, or dummy munitions; small electric explosive devices; fuel thickening compound; or items possessing other characteristics that clearly and positively negate potential use by terrorist, criminal, or dissident factions.

Source: US Department of Defense, Department of Defense Manual, No. 5100. 76, 2012c. http://www.dtic.mil/whs/directives/corres/pdf/510076m.pdf (accessed April 17, 2013).

Table 4.18 Casualty or Damage Risk Factor Values

Utility	*Risk Factor*	*Description*
High	1	Extremely damaging or lethal to personnel; devices that would probably cause death to personnel or major material damage
Moderate	2	Moderately damaging or injurious to personnel; devices that could probably cause personnel injury or material damage
Low	3	Temporarily incapacitating to personnel
None	4	Flammable items and petroleum-based products readily available from commercial sources

Source: US Department of Defense, Department of Defense Manual, No. 5100.76, 2012c. http://www.dtic.mil/whs/directives/corres/pdf/510076m.pdf (accessed April 17, 2013).

Table 4.19 Adaptability Risk Factor Values

Utility	*Risk Factor*	*Description*
High	1	Usable as is modification. Easy to employ with other system components.
Moderate	2	Slight modification. Other system components required; or can be used with slight modification.
Low	3	Major modification. Other components not available in the commercial market are required, or can be used with modification that changes the configuration.
Impractical	4	Requires specified functions or environmental sequences that are not readily reproducible, or construction makes it incapable of producing high-order detonation, for example, gas grains and impulse cartridges.

Source: US Department of Defense, Department of Defense Manual, No. 5100.76, 2012c. http://www.dtic.mil/whs/directives/corres/pdf/510076m.pdf (accessed April 17, 2013).

Table 4.20 Portability Risk Factor Values

Utility	*Risk Factor*	*Description*
High	1	Item easily carried/concealed by one person.
Moderate	2	Item that can be carried by one person for a short distance despite their shape, size, and weight.
Low	3	Items that require at least two persons to carry because of their shape, size, and weight.
Impractical	4	Material-handling equipment required. The weight, size, and shape of these items preclude the movement without material-handling equipment.

Source: US Department of Defense, Department of Defense Manual, No. 5100.76, 2012c. http://www.dtic.mil/whs/directives/corres/pdf/510076m.pdf (accessed April 17, 2013).

Table 4.21 Risk Factor Numerical Values and SRC Conversion

Numerical Rating (Sum Total from Decision Tables 3–6)	*Risk Factor Evaluation*	*SRC*[a]
(4–5)	High sensitivity	Item easily carried/concealed by one person.
(6–8)	Moderate sensitivity	Item can be carried by one person for a short distance despite its shape, size, and weight.
(9–12)	Low sensitivity	Item that requires at least two persons to carry because of its shape, size, and weight.
(13–16)	Nonsensitive	Material-handling equipment required. The weight, size, and shape of these items preclude the movement without material-handling equipment.

Source: US Department of Defense, Department of Defense Manual, No. 5100.76, 2012c. http://www.dtic.mil/whs/directives/corres/pdf/510076m.pdf (accessed April 17, 2013).

SRC I, man-portable missiles and rockets in a ready-to-fire configuration or when jointly stored or transported with the launcher tube and/or grip-stock and the explosive round, although not in a ready-to-fire configuration.

[a]SRC I calculation is not included as it is specifically defined.

4.5 CARVER Matrix

CARVER (acronym for *criticality*, *accessibility*, *recuperability*, *vulnerability*, *effect*, and *recognizability*) is used for rating the *relative desirability* of potential targets and for properly allocating attack resources. For every potential target, a lowest value of 1 to a highest value of 5 is assigned for each CARVER factor, thereby creating a CARVER matrix. Then, by totaling the six CARVER values, the total score for each target can be calculated; which represent the targets' relative prioritization. Moreover, the higher the CARVER score, the more significant a target becomes.

The CARVER matrix is a tool that evaluates the priority ranking of a given set of targets. The matrix also evaluates the strengths and weaknesses inherent in each target. The CARVER matrix for terrorism aimed on water infrastructures is presented in Tables 4.29 and 4.30.

Table 4.22 Criticality Values

Criteria	*Scale*
Immediate termination in outcome; target cannot function without it	9–10
Loss would reduce mission performance considerably, or two-thirds reduction in outcome	7–8
Loss would reduce mission performance, or one-third reduction in outcome	5–6
Loss may reduce mission performance, or 10% reduction in outcome	3–4
No significant effect on outcome	1–2

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

4.5.1 Criticality

Criticality is a target value and is the main component in targeting. A target is considered *critical* when its magnitude of destruction has a potential effect on military, political, or economic operations, or any operations of security and defense. The value of a target will change depending on the condition, requiring the use of time-sensitive methods to respond to the changing conditions. Criticality depends on several factors:

1. *Time*, which is crucial in evaluating the rapidness of the impact of destruction of a target that affects the operations
2. *The magnitude of outcome* due to target destruction
3. *The presence of substitutes* for the outcome product
4. *Perspective or relativity*, which is important in determining the number of targets and in evaluating their conditions

Table 4.22 shows how criticality values are assigned in CARVER matrixes.

4.5.2 Accessibility

A target is accessible when terrorists can physically intrude the target or if the target can be hit by direct or indirect methods. Accessibility varies with the intrusion/exit, the survival and escape potential of the target zone, the security situation, and the need for barrier penetration. The four basic steps identifying accessibility are

1. Intrusion from the staging base to the target zone
2. Movement from the point of entry to the target
3. Mobility to the target's critical object
4. The ability of the terrorist to escape

Table 4.23 Assigning Accessibility Values

Criteria	*Scale*
Easily accessible, standoff weapons can be used away from security	9–10
Inside a perimeter fence but outdoors or easily accessible outside	7–8
Easily accessible, inside a building or a structure but on ground floor	5–6
Difficult to gain access inside a building or a structure but easy on the top floor or in the basement; climbing or crawling required	3–4
Not accessible (very difficult to gain access)	1–2

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

The use of obstacle equipment and methods should always be considered when evaluating accessibility. The ability of the terrorists to survive is not usually associated with a target's accessibility. The factors considered when evaluating accessibility include, but are not limited to, the following:

1. Advance warning systems
2. Detection devices
3. Defense capabilities within the target zone
4. Transportation systems
5. Terrain and location
6. Concealment
7. Population density
8. Barriers
9. Weather conditions
10. Roadways

It is crucial to measure the time it could take for the terrorists to penetrate the barrier along each way based on the relative ease/difficulty of movement, and the likelihood of detection. Hence, the use of standoff weapons should be incorporated in the assessment. Table 4.23 shows how accessibility values are assigned on CARVER matrixes.

4.5.3 Recuperability

Recuperability is the period needed to recover or circumvent the destruction inflicted on the target. It varies with the source and type of targeted components and the availability of spare parts. Table 4.24 shows how recuperability values are assigned on CARVER matrixes.

Table 4.24 Assigning Recuperability Values

Criteria	*Scale*
Extremely difficult to replace, recovery requires 1 year or more	9–10
Difficult to replace or recover in less than 1 year	7–8
Can be replaced in a relatively short time (months)	5–6
Easily replaced in a short time (weeks)	3–4
Easily replaced in a short time (days)	1–2

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

4.5.4 Vulnerability

Vulnerability is a measure of the ability of the terrorists to destroy the target object, and the scale of the critical component needs to be compared with the ability of the terrorists to destroy (e.g., destruction of high-speed rail). The terrorists may tend to choose particular targets and cause permanent damage and maximize effects through the use of weapons, resulting in destruction of the targets (e.g., destruction of aqueducts). Table 4.25 shows how vulnerability values are assigned on CARVER matrixes.

Table 4.25 Vulnerability Values

Criteria	*Scale*
Vulnerable to long-range target designation; special operations forces definitely have the means and expertise to attack	9–10
Vulnerable to light weapons; special operations forces probably have the means and expertise	7–8
Vulnerable to medium weapons or very careful placement of smaller charges; special operations forces may have the means and expertise to attack	5–6
Vulnerable to special weapons; special operations forces probably have no impact	3–4
Invulnerable to all but the most extreme targeting measures; special operations forces do not have much capability to attack	1–2

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

Table 4.26 Assigning Effect Values

Criteria	*Scale*
Overwhelming negative effects; no significant positive effects; assured adverse impact on civilians	9–10
Moderate negative effects; few significant positive effects; adverse impact on civilians	7–8
No significant effects; neutral; some adverse impact on civilians	5–6
Moderate positive effects; few significant negative effects	3–4
Overwhelming positive effects; no significant negative effects, favorable sociological impact	1–2

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

4.5.5 Effect

The effect of an asset attack is a measure of possible security, military, political, environmental, and sociological impacts. The type and intensity of consequences will help analysts and decision makers select targets and target components for attack. Usually, the effect of a target attack includes the effect on the local population, but now effects also include

1. Triggering of countermeasures
2. Economic aftershocks
3. National panic and chaos
4. Collateral damage to other targets

Table 4.26 shows how effect values are assigned on CARVER matrixes.

4.5.6 Recognizability

An asset's *recognizability* is the level to which it can be identified and perceived by intelligence, survey, and exploration. Other factors that influence recognizability include the size, popularity, and complexity of the asset; the existence of distinctive asset signatures; and the technical sophistication and training of the terrorists. Table 4.27 shows how recognizability values are assigned on CARVER matrixes. Each element target is evaluated for each CARVER factor by entering the suitable value into the matrix. Once all the potential targets are evaluated, values for each potential target are added. The summation represents the relative desirability of each potential target, constituting a prioritized list of targets. Those targets with the highest totals are attacked first (Tables 4.28 and 4.29).

Table 4.27 Assigning Recognizability Values

Criteria	*Scale*
The target is clearly recognizable under all conditions and from a distance; it requires little or no training; easily recognized by all with no confusion.	9–10
The target is easily recognizable at small-arms range and requires a little training for recognition.	7–8
The target is difficult to recognize at night or in bad weather, or might be confused with other targets or target components; it requires some training for recognition; easily recognized by most, with little confusion.	5–6
The target is difficult to recognize at night or in worst weather condition, even within small-arms range; it is easily confused with other targets or components; it requires extensive training for recognition, hard to recognize, with probable confusion.	3–4
The target cannot be recognized under any condition, except by experts. Extremely difficult to recognize without extensive orientation.	1–2

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

4.6 CARVER + Shock

CARVER + Shock is a prioritization tool that can be used to assess the vulnerabilities within an infrastructure as detailed in Section 4.5, and a seventh attribute, *Shock*, has been incorporated with the original six elements to assess the combined health, environment, economic, cognitive reactions, and psychological impacts of an attack. Table 4.30 shows how shock values are assigned on CARVER + SHOCK. After the ranking on each of the attribute scales has been measured for a given node, the ranking on all the scales is added to give an overall value for that node. The nodes with the *highest overall rating have the highest probable risk and should be the focus of providing the preventive measures*. The process evaluations using this tool for pipelines, tunnels, rail, and transit systems are shown in Tables 4.31 and 4.32.

4.7 Model-Based Vulnerability Analysis

Scalable or model-based vulnerability analysis (MBVA) is an extensive tool of analysis that combines risk analysis, fault tree method, event tree method, and network analysis based on the principles of probability and cost minimization. The MBVA

Table 4.28 Strategic CARVER Matrix Application for Tunnels, Rail, and Transit Systems

Strategic CARVER Matrix							
Target Systems	*C*	*A*	*R*	*V*	*E*	*R*	*Total*
1. Oil and gas pipelines (*gathering lines and trunk lines*)	7	10	7	9	7	4	44
2. Aqueducts (water pipelines) considered as a *life blood* of large metropolitan areas in the United States	8	8	10	10	10	10	56[a]
3. Railroad/railway tunnels	10	9	10	10	10	9	58[a]
4. Underwater tunnels	10	4	8	8	10	10	50[a]
5. Road and highway tunnels	10	10	9	10	10	10	59[a]
6. Underground high-speed train (e.g., SwissMetro)	10	10	9	10	10	10	59[a]
7. Tubular rail system	8	8	4	9	9	10	48[a]
8. Underground freight transportation through pipelines and CargoCap	8	8	10	8	8	10	52[a]
9. Mine tunnel	8	8	9	8	8	10	51[a]

[a] Indicates target system suitable for attack.

Table 4.29 Operational CARVER Matrix Application for Tunnels, Rail, and Transit Systems

Operational CARVER Matrix							
Target Subsystems	*C*	*A*	*R*	*V*	*E*	*R*	*Total*
1. SCADA/cyber components	10	3	10	10	10	7	50[a]
2. Electrical controls	10	4	6	10	10	7	47[a]
3. Mechanical systems	10	4	6	10	10	7	47[a]
4. Floodgates	9	7	7	10	10	7	50[a]
5. Ventilation systems	9	7	7	7	9	6	45[a]
6. Walls/columns	9	9	9	6	8	10	51[a]
7. Rails	10	10	6	10	9	5	50[a]

[a] Indicates target system suitable for attack.

Table 4.30 Assigning Shock Values

Criteria	*Scale*
Target has major historical, cultural, religious, or other symbolic importance; loss of over 5000 lives; national economic impact more than $100 billion	9–10
Target has high historical, cultural, religious, or other symbolic importance; loss of between 500 and 5000 lives; national economic impact between $50 and $100 billion	7–8
Target has moderate historical, cultural, religious, or other symbolic importance; loss of between 150 and 500 lives; national economic impact between $5 and $50 billion	5–6
Target has little historical, cultural, religious, or other symbolic importance; loss of less than 150 lives; national economic impact between $50 million and $5 billion	3–4
Target has no historical, cultural, religious, or other symbolic importance; loss of less than 50 lives; national economic impact less than $50 million	1–2

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

was mostly used by computer science, network science, and information technology professionals and later on was adopted for homeland critical infrastructure risk/vulnerability analysis. In MBVA, hubs are identified, hub vulnerabilities are organized and quantified using fault tree, all possible events are organized as an event tree, and an optimal investment strategy is computed that minimizes risk (Lewis 2006). The primary procedure of MBVA includes the network analysis, which is basically rooted in the scale-free network theory, proposed by Derek J. de Solla Price in 1965, called *cumulative advantage* or *preferential attachment*. Albert-Laszlo Barabasi rediscovered and popularized the network theory in 1999. In this theory, critical infrastructure is modeled as a network, with nodes and links conceptually representing areas, power lines, power generators, cyber technologies, or sector assets and relationships among those assets. According to Ted G. Lewis (2006), vulnerability is not the same as risk; vulnerability is the probability of a risk event, whereas risk is measured in terms of financial risk, casualty risk, and equipment risk. Risk is the product of vulnerability V (probability ranging from 0 to 1.0) and cost D (an estimate of damages). Lewis stated that it is important to distinguish the calculation of vulnerability from that of risk, because vulnerability reduction achieves a different goal than risk reduction. Hence, Lewis is one of the authors in the field of homeland and critical infrastructure security who popularized MBVA. Generally, MBVA uses network analysis with fault tree modeling to

Table 4.31 Strategic CARVER + Shock Application for Tunnels, Rail, and Transit Systems

Strategic CARVER + Shock								
Target Systems	*C*	*A*	*R*	*V*	*E*	*R*	*Shock*	*Total*
1. Oil and gas pipelines (*gathering lines and trunk lines*)	7	10	7	9	7	4	4	48
2. Aqueducts (water pipelines) considered as a *life blood* of large metropolitan areas in the United States	8	8	10	10	10	10	7	63[a]
3. Railroad/railway tunnels	10	9	10	10	10	9	5	63[a]
4. Underwater tunnels	10	4	8	8	10	10	5	55[a]
5. Road and highway tunnels	10	10	9	10	10	10	5	64[a]
6. Underground high-speed train (e.g., SwissMetro)	10	10	9	10	10	10	7	66[a]
7. Tubular rail system	8	8	4	9	9	10	5	53[a]
8. Underground freight transportation through pipelines and CargoCap	8	8	10	8	8	10	3	55[a]
9. Mine tunnel	8	8	9	8	8	10	3	54[a]

[a] Indicates target system suitable for attack.

derive vulnerability, risk, and resource allocation strategies. Lewis, in his book, *Critical Infrastructure Protection in Homeland Security*, provides some specific presentation of the MBVA model for critical infrastructures.

4.8 Freight Assessment System

The Freight Assessment System (FAS) is designed to minimize the risks of potential terror threats to the nation and is associated with the estimated 50 billion pounds of domestic cargo transported annually by air carriers. Congress directed the Transportation Security Administration (TSA) in 2004 to develop a system to identify and target increased-risk cargo, and recently mandated the TSA to implement security plans to support a 50% screening of all cargo requirements by February 2009, and 100% screening of all cargo by August 2010. This new policy is called the *Certified Cargo Screening Program*, which is designed to connect via portals to TSA legacy and future systems to enable data transfer and receive risk-based

Table 4.32 Operational CARVER + Shock Application for Tunnels, Rail, and Transit Systems

Operational CARVER + Shock								
Target Subsystems (Using Explosives)	*C*	*A*	*R*	*V*	*E*	*R*	*Shock*	*Total*
1. SCADA/cyber components	10	3	10	10	10	7	5	55[a]
2. Electrical controls	10	4	6	10	10	7	1	48[a]
3. Mechanical systems	10	4	6	10	10	7	2	49[a]
4. Floodgates	9	7	7	10	10	7	6	56[a]
5. Ventilation systems	9	7	7	7	9	6	2	47[a]
6. Walls/columns	9	9	9	6	8	10	6	57[a]
7. Rails	10	10	6	10	9	5	2	52[a]

data. Additionally, FAS will eventually share crucial information with other modes of transportation: rail, highway, and motor carriers.

System-Based Risk Management Asset Assessment is used in the FAS, utilizing an analytical approach that seeks to develop technology and policy for preventive measures to reduce the risks to those assets that are critical to the sector's strategic risk objectives. Risk assessments carry a large boundary of interpretations that vary within industries. Moreover, the fundamental understanding of what properly constitutes the risk assessment process can vary. In the context of homeland security, risk assessments typically focus on threats, vulnerabilities, and consequences (TVC).

$$\text{Relative risk} = f(\text{threat},\ \text{vulnerability},\ \text{consequence}) \tag{4.3}$$

Separate analyses are associated with each term (e.g., threat analysis and vulnerability analysis). A set of activities representing the TVC analyses are input into a resulting risk assessment model. The output of a risk assessment model provides a relative scoring, either qualitative or quantitative, for the assets under analysis. This risk assessment authorizes the development of outcome-focused countermeasures designed to reduce the overall risk to the assets under study.

4.9 Federal Emergency Management Agency HAZUS-MH

HAZUS (HAZards United States) is a geographic information system–based natural hazard loss assessment model created by the Federal Emergency Management

Agency (FEMA). The current version is HAZUS-MH MR4, where MH stands for *multi-hazards*. Currently, HAZUS can model floods, hurricanes, and earthquakes. It is also used for mitigation and recovery as well as preparedness and response (FEMA 2013). Moreover, this tool can be implemented in terrorism risk assessment under special conditions due to the following key considerations:

1. It quantitatively identifies the exposure of a selected area.
2. It systematically characterizes the magnitude of the hazard affecting the exposed area.
3. It exploits the exposed area and the hazard to measure the levels of the potential losses.

4.10 Security Vulnerability Assessment

Risk of the security event is assessed qualitatively by the Security Vulnerability Assessment (SVA) by the National Petrochemical and Refiners Association (NPRA) and the American Petroleum Institute (API). The first step in the process of estimating risk is to identify and analyze the threats and the vulnerabilities facing a facility by an SVA. The SVA is a systematic process that evaluates the likelihood that a threat against a facility will be successful (API-NPRA 2004). The objective of conducting an SVA is to identify security hazards, threats, and vulnerabilities facing a facility and to evaluate the countermeasures for protecting the public, workers, national interests, the environment, and the facility (API-NPRA 2004). The basic approaches to estimate the potential risk are (1) deter, (2) detect, (3) delay, (4) deny, (5) defeat, and (6) respond.

Appropriate approaches for managing security vastly depend on the individual characteristics of the facility, including the type of facility and the threats facing the facility. Accordingly, in the SVA process, risk is a function of

1. Consequences of a successful attack against a facility
2. Likelihood of a successful attack against a facility

Likelihood is a function of

a. The attractiveness for the potential attack
b. The magnitude of the consequence
c. The degree of vulnerability of the asset

The SVA process does not recommend preventive measures but provides analysis and estimation of vulnerabilities. An example of the general SVA step screening process for water infrastructure is illustrated in Table 4.33, and the SVA ranking levels are presented in Table 4.34.

Table 4.33 General Steps of Security Vulnerability Assessment Screening Process

Screening Process
Step 1: Security risk definition based on the consequences and likelihood of an attainable attack against an asset. Some examples of significant consequences in an SVA include the following: Public health injuries Irreversible damage to aqueducts and underwater tunnels Public panic and chaos Loss of business viability Water shortage (short-term and long-term) Economic stress due to remediation cost Mass casualties Disruption of the downstream industry Long-term health effects Damage to the environment
Step 2: Likelihood definition based on the attractiveness of the asset to the terrorist, the degree of threat from terrorism, and the degree of vulnerability a. Asset attractiveness: Effect Potential for causing mass casualties Potential for damaging the environment Potential for creating public chaos Potential for damaging the regional or national economy Potential for massive media attention Potential for creating water shortage Target Chemical (and explosive) weapons Iconic targets Usefulness of the process material as a weapon Proximity to a national landmark

Table 4.33 (continued) General Steps of Security Vulnerability Assessment Screening Process

Screening Process
b. Threat:
Amateur terrorists/vandals
Disgruntled individuals
Self-radicalized individuals
Terrorists
Criminals
Activists
c. Vulnerability
Unsecured underground rail and transit systems (e.g., *SwissMetro, magnetic levitation train, CargoCap, and tubular rail*) (no sophisticated security system)
Weak economy that needed to lease the land above underground reservoirs (ASR)
Unsecured dam and reservoirs (no sophisticated security system)
Unsecured aqueducts
Weakness or poor relation between employees and management that caused a disgruntled individual within working facilities
Deficiencies in the protection policies for the water reserves such as aquifers

Source: Derived from American Petroleum Institute-National Petrochemical and Refiners Association., *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, 2nd edn., American Petroleum Institute, Washington, DC, 2004. http://www.npra.org/docs/publications/newsletters/SVA_2nd_edition.pdf (accessed August 14, 2010).

4.11 Automated Targeting System

The Automated Targeting System (ATS) is a DHS-computerized system that, for every individual person and cargo that crosses US borders, analyzes an ample volume of data which assigns a rating based on which the person may be considered in a risk group of terrorists or other criminals. Currently, ATS consists of six modules that focus on exports, imports, passengers and crew (airline passengers and crew on international flights, passengers and crew on sea carriers), private vehicles crossing land borders, and import trends over time (DHS 2006, 2007). ATS is consistent in

Table 4.34 SVA Ranking Levels

Ranking Levels	*Threat*	*Attractiveness*	*Vulnerability*
1—Very low	There is no plausible evidence of actual threats against the pipelines, tunnels, underground rail, and transit systems or other critical infrastructures.	No interest to attack pipelines, tunnels, underground rail, and transit system.	There are multiple layers of effective protective measures to the threat.
2—Low	There is a low threat.	Some interest.	There are effective protective measures in place within or surrounding the pipelines, tunnels, underground rail, and transit system; however, at least one weakness exists that an adversary would be capable of defeating the countermeasure.
3—Medium	There is a possible threat to pipelines, tunnels, underground rail, and transit systems based on the adversary's desire to compromise similar sectors.	Moderate interest in attacking the water infrastructure.	Although there are some effective protective measures, there is no complete and effective application of these security strategies to protect pipelines, tunnels, underground rail, and transit systems.

Table 4.34 (continued) SVA Ranking Levels

Ranking Levels	*Threat*	*Attractiveness*	*Vulnerability*
4—High	A potential threat exists based on capability of the adversary's intent to attack.	High-level interest of attacking the pipelines, tunnels, underground rail, and transit system.	There are some protective measures to deter, detect, delay, defeat, or respond to the pipelines, tunnels, underground rail, and transit systems but not a complete or effective application of these security strategies.
5— Very high	A plausible threat exists against pipelines, tunnels, underground rail, and transit systems, and that the adversary is capable of launching an attack.	Very high level interest in destruction of pipelines, tunnels, underground rail, and transit systems.	There are no effective protective measures currently in place to deter, detect, delay, defeat, and respond to the threat.

Sources: Derived from American Petroleum Institute-National Petrochemical and Refiners Association, *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, 2nd edn., American Petroleum Institute, Washington, DC, 2004. http://www.npra.org/docs/publications/newsletters/SVA_2nd_edition.pdf (accessed August 14, 2010); Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

its evaluation of risk associated with individuals and is used to support the overall Custom and Border Protection (CBP) law enforcement mission.

4.11.1 ATS-Inbound

ATS-Inbound is the primary decision support tool for inbound targeting of cargo and is available to CBP officers at all major ports (air/land/sea/rail) throughout the United States and assists CBP personnel in the Container Security Initiative decision-making process (DHS 2006, 2007).

4.11.2 ATS-Outbound

ATS-Outbound is the outbound cargo targeting of exports that pose a high risk of containing hazardous chemicals and violate Federal Aviation Administration rules. It utilizes Export Declaration data from CBP's automated export system.

4.11.3 ATS-Passenger

ATS-Passenger is used at all US airports and seaports receiving international flights and ships to evaluate and screen passengers and crew that can be a potential risk for creating danger to homeland or violating US law.

4.11.4 ATS-Land

ATS-Land (ATS-L) provides risk assessment of private passenger vehicles crossing the US border for security and screening by inspection of license plate numbers of vehicles. ATS-L permits CBP officers to compare information, evaluation of the assessment, and cross-reference the Treasury Enforcement Communications System (TECS) crossing data, TECS seizure data, and State Department of Motor Vehicle data for using weighted rule sets to provide risk scores.

4.11.5 ATS-International

ATS-International provides foreign customs authorities with controlled access to automated cargo-targeting capabilities (DHS 2006) and provides critical collaboration to other countries in enhancing the security of international supply chains and increasing protection from being disrupted by terrorists.

4.11.6 ATS-Trend Analysis and Analytical Selectivity

ATS-Trend Analysis and Analytical Selectivity allows CBP to examine, trace, identify, and target action violators of US laws regarding international trade. The trend analysis functions thoroughly review historical statistics that provide an overview of trade activity and provide support in determining illegal trade activity.

4.12 Sandia National Laboratories Security Risk Assessment Methods

A risk assessment process has been refined by Sandia National Laboratories to assess risk at various types of facilities and critical infrastructures. The method is based on the risk equation provided by Garcia (2008) in her book *The Design and Evaluation of Physical Protection Systems*:

$$\text{Risk} = P_A \times (1 - P_E) \times C \tag{4.4}$$

where

P_A is the likelihood of adversary attack
P_E is the security system effectiveness
$1 - P_E$ is the adversary success
C is the consequence of loss of the asset

The primary step in this risk assessment method is the characterization of the facility which includes identification of the undesired events and the respective critical assets. Guidelines for determining terror threats and for using the definition of the threat to estimate the probability of adversary attack against the facility are included. Hence, relative values of consequence and the effectiveness of the security system against the adversary attack are estimated.

4.13 ASME RA-S Probabilistic Risk Assessment

The American Society of Mechanical Engineers Probabilistic Risk Assessment Standard (ASME RA-S) is for non-light-water reactor nuclear power plant applications. The Probabilistic Risk Assessment (PRA) is a mainstream regulatory tool that contributes to the decision-making process for plant design, operation, and maintenance. Hence, the principle and standard of PRA can be applied in the PRA process for water infrastructure risk analysis.

In March 1999, the General Accounting Office (GAO) issued GAO/RCED-99–95, *Nuclear Regulation: Strategy Needed to Regulate Safety Using Information on Risk*. GAO stated that it is important to *develop standards on the scope and detail of risk analyses needed for utilities to determine that changes to their plants' design will not negatively affect safety*. The standard establishes requirements for a PRA ranging from a limited-scope to a *full-scope* PRA.

The meaning of *full scope* includes but is not limited to

1. Sources of radioactive material both within and outside the reactor core or system
2. The entire set of plant-operating states protecting all anticipated operating and shutdown modes
3. The entire set of initiating events (e.g., fires, floods, and seismic events); a definition of event sequences to a magnitude that is required to characterize mechanistic source terms and offsite radiological and chemical consequences to public health and safety
4. A measurement of
   a. The event sequence frequencies
   b. Mechanistic source terms

c. Offsite radiological and chemical consequences
d. Risk
e. Vulnerability
f. Associated uncertainties

Currently, ASME RA-S does not cover accidents resulting from acts of terrorism. However, the PRA standard procedure can be used as a guideline in risk analysis for terrorism occurring in pipelines, tunnels, underground rail, and transit systems because *the degree of consequences generated from a catastrophic nuclear power plant accident is comparable to the magnitude of consequences from terrorism* (e.g., the *psychological response* created by a nuclear power plant accident is almost equal to terrorism).

4.14 Development of Prospect Theory

Prospect theory is a theory of decision making under risk conditions deep-rooted in the *quantitative psychology of intuitive judgments*. Decisions are based on judgments under conditions of uncertainty, when it is difficult to clearly *foresee* the consequences of negative events. Prospect theory directly addresses how these preferences are framed and assessed in the decision-making development. Daniel Bernoulli was the first to introduce the concept of systematic bias in decision making based on a "psychophysical" model. Bernoulli used a coin toss game known as *St. Petersburg's Paradox* to demonstrate the limitations of expected value as a normative decision rule, which led him to analyze the *utility function* to explain people's choice of behavior (Kahneman and Tversky 1979). He assumed that people tried to maximize their utility and not their expected value. Bernoulli's function proposed that utility was not merely a linear function of wealth but rather a subjective evaluation of outcome (McDermott 1998). The concave shape of the function introduced the idea of declining minor utility, through which changes away from the starting point have less impact than those that are closer. For instance, Bernoulli's utility function argues that $1 is a lot compared with nothing; people will, therefore, be reluctant to part with this dollar. However, to most people, $101 is not significantly different from $100. Because Bernoulli's concave utility function assumes that increments in utility decrease with increasing wealth, the expected utility model implicitly assumes risk aversion (McDermott 1998). Thus, prospect theory is based on psychophysical models, such as those that originally inspired Bernoulli's expected value proposition. Tversky and Kahneman (1986) applied psychophysical principles to investigate intuitive prediction and decision-making analysis. People are not conscious of how the brain interprets vision into prospect. People make decisions based on how their brains comprehend fact or information and not exclusively on the basic utility that a certain choice obtains for a decision maker.

4.14.1 Expected Utility Theory

According to Kahneman and Tversky (1979), decision making under risk can be observed as a preference between prospects or gambles. A prospect $(x_1, p_1; \ldots; x_n, p_n)$ is a contract that yields an outcome x_i with probability p_i, where $p_1 + p_2 + \cdots + p_n = 1$. To simplify notation, we omit null outcomes and use (x, p) to denote the prospect $(x, p; 0, 1 - p)$, which yields x with probability p, and 0 with probability $1 - p$. The (riskless) prospect that yields x with certainty is denoted by (x) (Kahneman and Tversky 1979).

4.14.2 Prospect Theory

According to Kahneman and Tversky (1979), the *classical prospect theory* distinguishes two phases in the choice process: *framing* and *valuation*. In the *framing* stage, the decision maker develops a representation of the consequences that are crucial to the decision. In the *valuation* stage, the decision maker assesses the value of each prospect and chooses systematically. Then, the decision maker is considered to evaluate each of the refined prospects, and to select the prospect of highest value. The overall value of a refined prospect, designated as V, is expressed in terms of two scales, π and v. The first scale, π, associates a decision weight $\pi(p)$ with each probability, p, which reveals the influence of p on the overall value of the prospect.

4.15 Cumulative Prospect Theory

Prospect theory was modified by Kahneman and Tversky (2000) into cumulative prospect theory. The five foremost *phenomena of* choice, as detailed in Sections 4.16.1 through 4.16.5, which violated the standard model and put a basic challenge must be met by any adequate descriptive theory of choice (Kahneman and Tversky 2000).

4.15.1 Framing Effects

The rational theory of choice assumes description invariance: equivalent formulations of a choice problem should give rise to the same preference order (Arrow 1982). Contrary to this assumption, there is much evidence that variations in the framing of options yield systematically different preferences (Tversky and Kahneman 1986).

4.15.2 Nonlinear Preferences

According to the expectation principle, the utility of a risky prospect is linear in outcome probabilities. Allais's (1953) famous example challenged this principle by

showing that the difference between probabilities of 0.99 and 1.00 has more impact on preferences than the difference between 0.10 and 0.11. More recent studies observed nonlinear preferences in choices that do not involve sure things (Camerer and Ho 1994).

4.15.3 Source Dependence

People are eager to bet on an uncertain event based on the magnitude of uncertainty and on its source or cause. More recent evidence indicates that people often prefer to bet on an event although the former probability is vague and the latter is clear (Heath and Tversky 1991).

4.15.4 Risk Seeking

Risk aversion is immediately assumed in economic analysis of decision under uncertainty. It is a behavior when a person exposed to uncertainty will try to minimize that uncertainty or avoid unnecessary risk. Thus, the decision maker has a different point of view of the value of a risky alternative versus the value of the alternative due to the negative impacts of risk by the alternative.

4.15.5 Loss Aversion

One of the basic phenomena of choice under both risk and uncertainty is that losses loom larger than gains (Tversky and Kahneman 1991). A person evaluates risk preferring to avoid losses to attaining gains.

4.15.6 Cumulative Prospect Theory

The new theory explains loss aversion, risk seeking, and nonlinear preferences in terms of the value and the weighting functions (Kahneman and Tversky 2000). In cumulative prospect theory as defined by Kahneman (2000), S is a definite set of states of nature (subsets of S are called "events"). X is a set of consequences or "outcomes." Assume X is a neutral outcome, denoted as 0. All other elements of X are gains (+) or losses (–). A prospect f is then represented as a sequence of pairs (x_i, A_i), which yields x_i if A_i occurs, where $x_i > x_j$ iff $i > j$ and (A_i) is a partition of S. The positive part of f, denoted as f^+, is obtained by

$$f^+(s) = f(s) \quad \text{if} \quad f(s) > 0$$

$$f^+(s) = 0 \quad \text{if} \quad f(s) \leq 0$$

The negative part of f, denoted as f^-, is defined similarly.

Based on Kahneman and Tversky (2000), existing increasing value function, $v{:}X \rightarrow Re$, satisfying $v(x_0) = v(0) = 0$, and capacities W^+ and W^-, such that for $f = (x_i, A_i), -m \leq i \leq n$,

$$V(f) = V(f^+) + V(f^-) \tag{4.5}$$

$$V(f^+) = \sum_{i=0}^{n} \left(\pi_i^+ v(x_i)\right) \tag{4.6}$$

$$V(f^-) = \sum_{i=m}^{n} \left(\pi_i^- v(x_i)\right) \tag{4.7a}$$

where the decision weights $\pi^+(f^+) = (\pi_0^+, \ldots, \pi_n^+)$ and $\pi^-(f^-) = (\pi_{-m}^-, \ldots, \pi_0^+)$ are defined by

$$\pi_n^+ = W^+(A_n), \quad \pi_{-m}^- = W^-(A_{-m})$$

$$\pi_i^+ = W^+(A_i \cup \cdots \cup A_n), -W^+(A_{i+1} \cup \cdots \cup A_n)$$

Letting $\pi_i = \pi_i^+$ if $i \geq 0$ and $\pi_i = \pi_i^-$ if $i < 0$, Equations 4.7a and 4.7b reduce to

$$V(f^+) = \sum_{i=-m}^{n} \left(\pi_i^+ v(x_i)\right) \tag{4.7b}$$

The decision weight π_i^+, in relation to a positive outcome, is the difference between the capacities of the events: "the outcome is at least as good as x_i" and "the outcome is at least as bad as x_i" (Kahneman and Tversky 2000). The decision weight π_i^-, associated with negative outcome, is at least as bad as x_i and is strictly worse than x_i (Kahneman and Tversky 2000). Thus, the decision weight associated with an outcome can be deduced as W^+ and W^-. It follows readily from the definitions of π and W that for both positive and negative prospects, the decision weights add to 1 and for mixed prospects, the sum can be either lesser or greater than 1 as defined by individual weights (Kahneman and Tversky 2000):

$$\pi_n^+ = \omega^+(p_n), \quad \pi_{-m}^- = \omega^-(p_m)$$
$$\pi_i^+ = \omega^+(p_n + \cdots + p_n) - \omega^+(p_{i+1} + \cdots + p_n), \quad 0 \leq i \leq n-1$$
$$\pi_i^- = \omega^-(p_{-m} + \cdots + p_i) - \omega^-(p_{-m} + \cdots + p_{i-1}), \quad 1-m \leq i \leq 0$$

where ω^+ and ω^- are increasing functions from the unit interval, $\omega^+(0) = \omega^-(0) = 0$, and $\omega^+(1) = \omega^-(1) = 1$.

According to Kahneman and Tversky (2000), cumulative prospect theory broadens the original theory as follows:

1. It applies to any controlled or limited prospect and it can be extended to continuous distributions.
2. It applies to both probabilistic and uncertain prospects and can coordinate some form of source dependence.
3. The improved theory allocates different decision weights for gains and losses, thereby simplifying the initial version that assumes $\omega^+ = \omega^-$.

Consequently, the cumulative prospect theory presented herein will be integrated into risk acceptability analysis as detailed in Chapters 6 and 7.

4.16 Conclusion

The risk and vulnerability assessment tools in this chapter are mostly utilized by experts and governmental agencies. The risk assessment and management methodologies found in the *NASA Systems Engineering Handbook* are used by most governmental agencies and experts in the security and defense field. However, it is more important to recognize that *perceived risk levels* may have far more to do with the acceptability based on the *quantitative psychology* of a protection policy formulation and preventive measures than the actual risk levels themselves. While developing policy and countermeasures, the *perspective views* of the public who are exposed and/or feel they are vulnerable and exposed to risks are significant in the consideration of the *systemic control* developments. It is critical to involve those people who are impacted by the policy and program choices to precisely deliver the facts on actual risks to which they are involved, when the exposure to the risk is *perceived as involuntary* such as with a *man-made disaster*: the process of making a decision considerably participatory heightens the nature of the risk being *voluntary*. Chapters 5 through will provide the readers with the probabilistic risk assessment model and *risk acceptability* analysis applications to pipelines, tunnels, underground rail, and transit systems.

References

Allais, M. 1953. Le comportement de l'homme rationnel devant le risqué, critique des postulats et axioms de l'Ecole Amercaine. *Econometrica* 21:503–546.

American Petroleum Institute–National Petrochemical and Refiners Association. 2004. *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, 2nd edn., Washington, DC: American Petroleum Institute. http://www.npra.org/docs/publications/newsletters/SVA_2nd_edition.pdf (accessed August 14, 2010).

American Society of Mechanical Engineers Innovative Technologies Institute, LLC. 2009. *All-Hazards Risk and Resilience Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach*. New York: ASME.

Arrow, K. J. 1982. Risk perception in psychology and economics. *Econ. Inquiry* 20:1–9.

Camerer, C. and Ho, T.H. 1994. Violations of the betweenness axiom and nonlinearity in probability, *Journal of Risk and Uncertainty*, Vol 8, Issues 2, pp 167–196.

Doro-on, A. 2011. *Risk Assessment for Water Infrastructure Safety and Security*. Boca Raton, FL: CRC Press.

Garcia, M. L. 2008. *The Design and Evaluation of Physical Protection Systems*, 2nd edn., Newton, MA: Butterworth-Heinemann.

Heath, C. and Tversky, A. 1991. Preference and belief: Ambiguity and competence in choice under uncertainty. *J Risk Uncertain*, 4:5–28.

Joint Interoperability Test Command. 2013. JITC risk assessment methodology. http://jitc.fhu.disa.mil/cgi/jsr/downloads/nrkpp_guidebook_appdxe.pdf (accessed April 17, 2013).

Kahneman, D. (2000). *Experienced utility and objective happiness: A moment-based approach*. In: D.Kahneman & A. Tversky (Eds.), Choices, values and frames. New York: Cambridge University Press and the Russell Sage Foundation. pp. 673–692.

Kahneman, D. and Tversky, A. 1979. Prospect Theory: An analysis of decision under risk. *Econometrica* 47(2):263–292.

Kahneman, D. and Tversky, A. 2000. *Choices, Values and Frames*. New York: Russell Sage Foundation and Cambridge University Press.

Lewis, T. 2006. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, NJ: John Wiley & Sons.

McDermott, R. 1998. *Risk Taking in International Politics-Prospect Theory in American Foreign Policy*. Ann Arbor, MI: University of Michigan Press. http://press.umich.edu/pdf/0472108670.pdf (accessed December 5, 2007).

National Aeronautics and Space Administration. 2007a. NASA system engineering manual. http://www.acq.osd.mil/se/docs/NASA-SP-2007–6105-Rev-1-Final-31Dec2007.pdf (accessed on February 23, 2013).

National Aeronautics and Space Administration. 2007b. Exploration systems: Risk management plan. http://www.nasa.gov/pdf/413721main_ESMD-RMP-04.06_Rev_2_FINAL.pdf (accessed February 23, 2013).

National Aeronautics and Space Administration. 2010. Technical probabilistic risk assessment (PRA) procedures for safety and mission success for NASA programs and projects. http://nodis3.gsfc.nasa.gov/npg_img/N_PR_8705_005A_/N_PR_8705_005A_.pdf (accessed April 17, 2013).

National Aeronautics and Space Administration. 2011. NASA risk management handbook. http://www.hq.nasa.gov/office/codeq/doctree/NHBK_2011_3422.pdf (accessed February 23, 2013).

Tversky, A. and Kahneman, D. 1986. Rational Choice and the Framing of Decisions, *The Journal of Business* 59(4), part 2, S251–S278.

Tversky, A. and Kahneman, D. 1991. Loss Aversion in Riskless Choice: A Reference Dependent Model, *Quarterly Journal of Economics* 107(4), 1039–1061.

US Department of the Air Force. 2003. Guidelines for successful acquisition and management of software-intensive systems: Weapon systems command and control systems management information systems. http://www.stsc.hill.af.mil/resources/tech_docs/gsam4.html (accessed April 17, 2013).

US Department of Defense. 2006. *Risk Management Guide for DOD Acquisition*, 6th edn., Fort Belvoir, VA: Department of Defense. http://www.acq.osd.mil/damir/documents/DAES_2006_RISK_GUIDE.pdf (accessed August 18, 2012).

US Department of Defense. 2012a. DOD counterfeit mitigation update. http://www.dscc.dla.mil/downloads/psmc/Apr12/5AntiCounterfeiting.pdf (accessed April 17, 2013).

US Department of Defense. 2012b. Department of defense instruction, No. 5200.44. http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf (accessed April 17, 2013).

US Department of Defense. 2012c. Department of Defense Manual, No. 5100.76. http://www.dtic.mil/whs/directives/corres/pdf/510076m.pdf (accessed April 17, 2013).

US Department of Defense. 2013. Risk management. http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseAmericasSecurityAffa/DefenseCriticalInfrastructureProgram/Risk.aspx (accessed April 17, 2013).

US Department of Homeland Security. 2006. Privacy impact assessment for the automated targeting system. Custom and Borders Protection, ATS, November 22, 2006. http://dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf (accessed June 3, 2010).

US Department of Homeland Security. 2007. Privacy impact assessment for the automated targeting system. Custom and Borders Protection, ATS, August 3, 2007. http://dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf (accessed June 3, 2010).

US Federal Emergency Management Agency. 2013. HAZUS. http://fema.gov/plan/prevent/hazus/ (accessed April 22, 2013).

Chapter 5

Quantitative Risk Estimation Model for Pipelines, Tunnels, Underground Rapid Rail, and Transit Systems

5.1 Introduction

This chapter demonstrates *quantitative risk estimation processes* for terrorism and disaster in oil and gas pipelines, tunnels, high-speed rail, and transit systems. One of the main examples focuses on the freight pipeline system using magnetic levitation (*maglev*) and linear electric induction motor for underground freight transshipment in pipelines. Examples related to clandestine tunnels for illegal manpower mobilization and fabrication of weapons of mass destruction (WMD) are included in the analysis. The idea of using *maglev* and other underground freight in capsules through tunnel systems is considered a futuristic advanced transportation technology for critical and hazardous goods in fragile or overpopulated areas, to be a viable alternative to congesting highways. Moreover, descriptive models are presented involving terrorist attacks using explosive devices that are difficult to mitigate or detect. This chapter will center on human safety, and environmental and economic consequences triggered by terrorism.

Risk can be described in a mathematical method as a function of the probability of occurrence of an adverse consequence and the value of that consequence. Therefore, the aspects required to prepare a risk estimation model include the joint probability of a series of events leading to the consequence, the value of this consequence, and the functional relationship defining risk. Risk has two major components: (1) the existence of a possible unwanted consequence or loss; and (2) an uncertainty in the occurrence of that consequence, which can be expressed in the form of a probability of occurrence (Rowe 1977). The evaluations of consequences include extensive probabilistic *risk estimation models*, *fault tree analysis*, and *event tree analysis*; details of these models are thoroughly presented in Chapter 7.

5.2 Elements of Risk Assessment

The array of risks covers a wide variety of human experiences involving risks, personal or societal, man-made or natural, with consequences ranging from financial involvement to premature death (Rowe 1977). Three major analytical steps in risk assessment are applied:

- Risk identification involves reduction of descriptive uncertainty (whereas risk reduction means risk is reduced to some acceptable level). At this level, we only cover the risk estimation process.
- Risk estimation is based on the systematic evaluation of probability values associated with events having negative consequences.
- Risk acceptability analysis is based on the quantitative revealed preferences method.

Further, the emphasis on risk acceptability analysis is presented in Chapter 6.

5.2.1 Risk Estimation Development for Terrorism against Pipelines, Rails, and Tunnels

Evidently, there is a deficiency and very limited strategic processes, technology, and regulations are being implemented for the protection of oil and gas pipelines, railways/railroads, underground freight transshipment through pipelines, and transit and tunnel systems. These are infrastructures *accessible or vulnerable to terrorist attacks using explosive devices* or other man-made disasters, not only in the United States but also in other countries. As proven in Iraq and Afghanistan, explosive devices (*commonly known as improvised explosive devices, IEDs*) are difficult to intercept and generated casualties of American soldiers and civilians. The following reasons delineate the possibility of successful terrorism:

- Inadequacy of appropriate technologies (e.g., intelligent detection and defense devices to counter explosive devices) and intuitive techniques for infrastructure protection and defense against improvised weapons.
- Pipelines, aqueducts (water supply pipelines), transit, and rail systems are constructed with great lengths and are mostly situated in remote areas and distant from populated areas, so there are tendencies that owners, decision makers, and stakeholders may likely overlook the security demands of these infrastructures.
- Most oil and gas pipelines are located in areas with higher risks of terrorism and vandalism.
- Obviously, oil and gas pipelines are susceptible to man-made disasters due to deficiency in protection policy and lack of sophisticated technology against explosive devices.
- Lack of *intelligent devices* to deter and defend the infrastructures against any illegal intrusion or sabotage.
- Deficiency in regulations enforcing effective *protective systems* against terrorism or other man-made disaster.
- Insufficient security surveillance on the vicinity adjacent to or neighboring these infrastructures.

5.2.2 Risk Estimation Development for Clandestine Fabrication and Transshipment of Weapons of Mass Destruction by Terrorists and Rebellious States to Endangering Homeland Security

For several decades, rebellious states and terrorists have been illegally constructing subterranean infrastructures and underwater technologies for secret operations to develop WMD for use in future conflicts and attacks to homeland, allies, and friendly nations. Ample evidence of tunnels built for secret *terror-military actions* and manufacturing of WMD recently surfaced through public media. Even advanced technologies were currently being launched and tested by these rebellious nations. The ancient Chinese philosopher/strategist, Sun Tzu, urged: "Know thy self, know thy enemy. A thousand battles, a thousand victories (Bennett 2012)." Because most of the adversaries' illegal secret activities were done in man-made subterranean infrastructures, it is truly difficult to predict these potential terror acts, and imposing regulations is not effective at all. There are a few *conceptual reasons* why the enemies and rebellious nations have attained success in producing WMD against homeland, allies, and friendly nations:

- Lack of hard evidence to convince international regulators and agencies that the enemies were able to negotiate and acquire weapon materials from other corrupt nations or organizations.

- Lack of hard evidence to validate the enemies' *devious motives* from developing these potential WMD technologies. If strong proof existed that these nations and terrorists acquired WMD materials, proving their secret motives to be harmful to national and international security is not simple.
- Deficiency in international policy and security to prevent *illegal* commerce, transshipment, and production of WMD materials.

For developing a risk estimation model, there are five steps: (1) causative event, (2) outcome, (3) exposure, (4) consequence, and (5) value of consequence. These five steps of the risk estimation process for terrorist attacks on infrastructures and secret operations are elaborated in Tables 5.1 and 5.2.

The causal relationship presented in Figure 5.1 illustrates how vulnerabilities of underground freight transportation might be exploited to result in such negative consequences.

5.3 Event Tree Analysis

Event trees and decision trees are inductive logic methods for identifying the various possible outcomes of a given initiating event, but they differ depending upon whether human control can influence the outcomes (as in decision trees) or whether the outcomes depend only upon the laws of science (as in event trees) (McCormick 1981). The initiating event in a decision tree typically is a particular risk acceptance decision, and the various outcomes depend upon subsequent decisions (Raiffa 1968, Tribus 1969). In risk assessment applications, the initiating event of an event tree is typically a system failure, and the subsequent events are determined by the system characteristics (Fussell and Arendt 1979). Event tree analysis is a logical tracing of sequential events resulting in consequential outcomes. An event tree begins with a defined accident-initiating event (McCormick 1981). This process imposes that the fundamental events and decision nodes in each complicated model originate from an initial event, resulting in various terminal outcomes, which are certainly recorded sequentially from cause to result. Diverse event trees must be developed depending on the condition and situation for analyzing a set of undesirable events. In Figure 5.2, A might be permitting underground freight transportation through tunnels (UFTT), where A0 would then be regarded if the UFTT were not constructed, resulting in a terminal node with the end result of no environmental impacts or contamination as a consequence of permitting UFTT. The A1 branch would then represent the implementation of UFTT construction plans. The B event node might then represent incorporation of the UFTT as a transshipment system of a hazardous cargo, options presented by this transitional node being no B0 or yes B1, and so on. Events are subsequently aggregated at the terminal end until all risk pathways are described.

Table 5.1 Process of Risk Estimation for Pipelines, Tunnels, Rail, and Transit Systems

Step 1: Causative events	
a.	Terrorists intrusion to oil and gas pipeline vicinities
b.	Terrorists intrusion to underground freight transportation through pipelines, *CargoCap*, and *maglev*
c.	Terrorists intrusion to tubular rails
d.	Terrorists intrusion to major stations of underground high-speed mass transit
e.	Terrorists intrusion to tunnel systems near populated/urban areas (e.g., road tunnels, rails, underwater/immersed tunnels, and drainage tunnel)
f.	Terrorists intrusion to aqueducts
Step 2: Outcome	
a.	Placing of explosive devices at tunnel surfaces and outlets
b.	Placing of WMD in *tubular rails* and *maglev* operating in overpopulated areas or within large metropolitan areas
c.	Freight transportation pipeline rupture
d.	Using explosive devices to severely rupture oil and gas pipelines
e.	Destruction of aqueduct structures by explosive devices
f.	Placing chemical threats and explosive devices in tunnel systems
g.	Ignition of flammable material to freight system or CargoCap
h.	Generate rail derailment and collision
i.	Generate electromechanical failure and cyber-controller system failure
Step 3: Exposure	
a.	*Chemical threats dispersion in the environment after the explosion of transit systems (i.e., maglev, and tubular rails)*: i. Chemical threats mixed in the atmosphere and the environment ii. Chemicals will not be treated easily iii. Chemicals mixed with other pollutants present in the environment iv. Chemicals diluted in some areas by strong winds

(*continued*)

Table 5.1 (continued) Process of Risk Estimation for Pipelines, Tunnels, Rail, and Transit Systems

b.	*The release of HAZMAT in the environment after oil and gas pipelines rupture*: i. HAZMAT contaminates the water bodies and soils of the surrounding environment after explosion ii. HAZMAT will not be treated immediately
c.	*Explosions of transit systems (i.e., maglev and tubular rails) created by explosive devices*: i. Derailment and rupture of maglev and tubular rails ii. Missiles in flight from transit/rail system burst iii. Generate flash fires and fireballs iv. Dust and fragment explosions
d.	*Flash flood after explosion of aqueducts*: i. Floodwater from aqueducts destroy the surrounding environment
e.	*Explosions of tunnel systems due to rail systems collision and release of flammable liquids*: i. Generation of debris and environmental contamination ii. Generation of flammable gas and liquid
f.	*Rupture of underwater tunnels*: i. Flash flood in underwater tunnels affecting the adjacent areas
g.	*Rupture of rails and freights after strong collisions*: i. Flash and pool fires during rail system disasters
Step 4: Consequence	
a.	Catastrophic health effects: Short-term effect: Death Long-term effects: Impaired human health (impaired immune functions, cause various cancers, and radiation poisoning)
b.	Disrupt downstream commercial agriculture and industry infrastructure due to aqueduct destruction: i. Flood and contaminate the environment ii. No other immediate water supply available after the attack
c.	Injury to the environment due to the release of missiles and debris

Table 5.1 (continued) Process of Risk Estimation for Pipelines, Tunnels, Rail, and Transit Systems

d.	Result in economic distress due to the tremendous need for reconstruction of infrastructures and environmental remediation
e.	Cause damage to public morale and confidence
f.	Number of casualties and sever injuries after bursting of missiles
g.	Mass casualties
h.	Pollute the environment and cause destruction of natural resources dependent on clean environment (after the release of toxic substance)
i.	Collapse of key transportation and freight system infrastructures
j.	Result in economic distress due to the need for emergency response and recovery after damaging oil and gas pipelines
k.	Result in economic distress due to the need for reconstruction and recovery after damaging rail tunnel systems
Step 5: Consequence values	
a.	Protection and security policy revision
b.	Provide detection, intrusion, and surveillance technology
c.	Improve intelligence
d.	Provide funding for research on improving technology and policy
e.	National security improvements
f.	Development of intelligent devices and technologies for security and defense approaches

In the step of expanding public safety and environmental protection model, the following top-level policies are analyzed:

1. A0: No terrorism worry (public safety and the environment are designated as protected)
2. A1a: Complete protection of the entire adjacent infrastructures and surrounding area or environment with a sophisticated fence and surveillance
3. A1d: Partial protection
4. A1e: Business as usual, no protection against terrorism

Using the event tree as a segment, the fault tree can be easily developed.

Table 5.2 Process of Risk Estimation for Clandestine Tunnels and Transshipment of WMD Materials

Step 1: Causative events	
a.	Terrorists/rebellious nations constructed secret tunnels near overpopulated (metropolitan) areas
b.	Terrorist/rebellious nations constructed secret infrastructures near or adjacent to underground freight transportation through pipelines, or *maglev* trains, to aid their manpower mobilization and terror operations and use those as a disguise system
c.	Terrorists/rebellious nations built friendly relationships with other corrupt nations
d.	Terrorists/rebellious nations secretly negotiated with other corrupt organizations/nations to acquire WMD materials, manpower mobilization, and hidden transport of WMD materials. *They successfully developed powerful WMD and its components without being interrupted during fabrication*
e.	Terrorists/rebellious nations installed cover-up systems to hide illegal operations
f.	Terrorists/rebellious nations constructed cross-border tunnels with other corrupt organizations for WMD materials and manpower transshipments
g.	Terrorists/rebellious nations constructed "escape" infrastructures to protect their terrorist and devious leaders after the terror attacks
Step 2: Outcome	
a.	Preparing terror-military operations against homeland, allies, and friendly nations
b.	Preparing security and defense systems for a successful launch of terror-military operations and WMD attacks
c.	Preparing effective secret WMD launch sites for attacks
d.	Preparing intrusion and attack positions

Table 5.2 (continued) Process of Risk Estimation for Clandestine Tunnels and Transshipment of WMD Materials

Step 3: Exposure	
a.	*Chemical threats/radioactive material dispersion in the environment after the WMD attacks*: i. Chemical threats/radioactive material mixed in the atmosphere and the environment ii. Chemical threats/radioactive material will not be treated immediately iii. Chemical threats/radioactive material diluted in some areas via strong winds
b.	*Explosion of infrastructures after the attacks*: i. Escape and burst of hazardous debris and gas from the collapse of infrastructures contaminated in the surrounding environment ii. Hazardous debris, missiles, and gas will not be treated immediately
c.	*Flash floods if large water reservoirs and pipelines are destroyed by WMD explosion*: i. Flush floods gushing toward the downstream areas
d.	*Detonation of WMD*: i. Lethal energy, radiant heat, and shock waves released ii. Abrupt flash and pool fires and jet flames released to the environment iii. Flash burns
Step 4: Consequence	
a.	Catastrophic health effects: i. Short-term effect: Death ii. Long-term effects: Impaired human health such as the development of various cancers, radiation poisoning, horrible burns, and untreatable *disease X* (*emergence of blue soars on body parts, vomiting, bleeding, diarrhea, and swollen body parts*)
b.	Disrupt all industry infrastructures after WMD attacks: i. Contaminate the environment ii. No other immediate water, food, and medical supplies available after the WMD attacks

(*continued*)

Table 5.2 (continued) Process of Risk Estimation for Clandestine Tunnels and Transshipment of WMD Materials

c.	Destruction and injury to the environment due to the release of radioactive material, other HAZMAT, and debris
e.	Result in economic distress due to the tremendous requirement for reconstruction of infrastructures, environmental remediation, recovery, and emergency medical supplies
f.	Cause damage to public psychology, morale, and confidence
g.	No other immediate medical supplies and no immediate medical health facilities available because they are mostly destroyed after WMD attacks
h.	Mass casualties
i.	Destruction of preserved resources
j.	Collapse of major infrastructures critical to national economy and public safety
Step 5: Consequence values	
a.	Revise protection and security policy (national and international). Enhance international collaborations
b.	Develop intelligent devices and technologies to mitigate illegal operations
c.	Provide funding for research on improving technology and policy. Improve decision-making process in choosing research and technological projects
d.	Incorporate and practice intuitive judgments and sound predictions to stakeholders, decision-makers, analysts, and engineers
e.	Improve intelligence

5.4 Estimation of Risk and Risk Factors

There are several methods for illustrating and evaluating risk data. At this point, two methods are widely used: (1) computation of risk rates and (2) computation of losses to life expectancy. There are also many approaches of acquiring and comparing risk rates for terrorist attacks on water infrastructure such as risk rates/factors based on fatal transportation accidents or nuclear power plant accidents using the two methods of computing risk rates and losses to life expectancy and risk rates/factors based upon intuitive judgment.

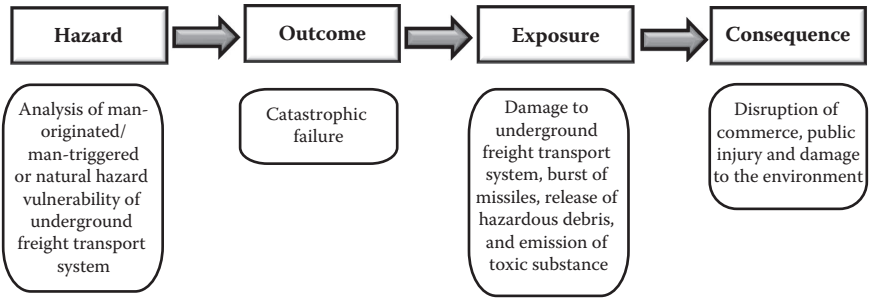


Figure 5.1 Conceptual model of risk pathway.

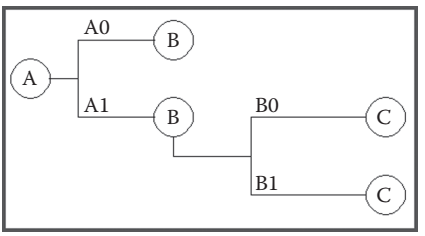


Figure 5.2 Example event tree.

The vulnerability of an infrastructure or its system component is estimated using the probability scale in decimal description provided in Table 5.3. This estimates the potential terrorism or disaster occurrence of the given events from the event tree analysis. Categories 3 and 4 are further subdivided to provide more refinement as the likelihood of success approaches to 1.0. This allows the owner, decision-maker, or analyst to intuitively measure changes in security and defense level. Infrastructure evaluations will depend upon the judgment of an expert based on experience and knowledge.

5.4.1 Calculation of Risk Rate

For a particular class of events i, such as motor vehicle accidents or commercial passenger aircraft accidents, a number of such accidents or events N_i will occur in a given period of years t_i. The mean number of accidents per year, $\overline{N}$, is computed by the formula

$$\overline{N} = \frac{N_i}{t_i} = \text{Mean number of accidents or events per year}$$

Table 5.3 Probability Scale Used for Critical Infrastructure Analysis Risk Estimation Model

Probability Scale for Critical Infrastructure and Key Resources Protection Analysis		
Category	*Description*	*Probabilities in Decimal Description*
4	Very high (*indicates that there are no effective policies or protective and defensive measures currently in place to deter, detect, delay, and respond to the threat*)	0.90–1.00
	High (*there are some policies and protective and defensive measures to deter, detect, delay, or respond to the asset but not a complete or effective application of these security strategies*)	0.80–0.89
		0.71–0.79
3	Medium high	0.61–0.70
	Medium low (*indicates that although there are some effective policies and protective and defensive measures, there is no complete and effective application of these security strategies*)	0.40–0.60
2	Low (*indicates that there are effective protective and defensive measures in place; however, at least one weakness exists that an adversary would be able to defeat the countermeasure*)	0.20–0.398
		0.10–0.198
1	Less likely—very low probability (*indicates no credible evidence of capability*)	0.05–0.099
		0.025–0.049
		<0.024

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.

For each event j, of class I, there will be a number of consequence measures for consequences of different nature:

F_{ij} is the number of total fatalities for accidents ij
F_{ij1} is the number of total fatalities under voluntary risk conditions
F_{ij2} is the number of total fatalities under involuntary risk conditions
I_{ij} is the number of total injuries
I_{ij1} is the number of total injuries, voluntary risk
I_{ij2} is the number of total injuries, involuntary risk
D_{ij} is the cost of event in dollars

Other dissimilar consequences (illness, quality of life factors, etc.) can all be addressed in the same manner as long as clear definitions exist:

$$F_{ij1} + F_{ij2} = F_{ij}$$
$$I_{ij1} + I_{ij2} = I_{ij}$$

The mean number of fatalities, injuries, or costs is obtained for each factor by taking the sum of the magnitude of each event and dividing it by the number of events in question. Thus

$\overline{F} = \frac{1}{N_i} \sum_j F_{ij}$ = Mean number of fatalities, per accident of type i
$\overline{F} = \frac{1}{N_i} \sum_j F_{ij1}$ = Mean number of fatalities, voluntary risk
$\overline{F} = \frac{1}{N_i} \sum_j F_{ij2}$ = Mean number of fatalities, involuntary risk

In the same manner, the mean number of injuries $\overline{I}_i$, $\overline{I}_{i1}$, and $\overline{I}_{i2}$ and the mean cost D_i can be calculated. Whether the mean (as opposed to the mode) is a good central measure depends on particular distributions of frequency and magnitude of events. If the frequency of events is high enough to provide some measure of statistical convergence, rates of fatalities, injuries, and costs can be computed for individuals and populations at risk. The populations at risk are denoted as follows:

P_i is the total population at risk
P_{i1} is the population subject to voluntary risks
P_{i2} is the population subject to involuntary risks

Then the number of fatalities, injuries, and costs per year for each class of accident or event N_i is of the form

$\overline{N}_i \times \overline{F}_i$ = Mean number of fatalities per year
$\overline{N}_i \times \overline{I}_i$ = Mean number of injuries per year
$\overline{N}_i \times \overline{D}_i$ = Mean year costs

The risk to an individual is

$\overline{f_i} = \frac{N_i \times F_i}{P_i}$ = Mean probability of death to an individual at risk per year
$\overline{k_i} = \frac{\overline{N_i} \times \overline{I_i}}{P_i}$ = Mean probability of injury to an individual at risk per year

The death rate per 100,000 people at risk f_i is

$$f_i = \overline{f_i} \times 10^5 = \frac{N_i \times \overline{F_i} \times 10^5}{\overline{P}_i}$$

And injury rate per 100,000 people at risk k_i is

$$k_i = \overline{k_i} \times 10^5 = \frac{N_i \times \overline{I}_i \times 10^5}{\overline{P_i}}$$

The voluntary and involuntary risk rates can be found accordingly.

The use of the population at risk as a divisor involves some danger of misrepresentation. Meanwhile, the larger the population at risk, the smaller is the individual risk for a given consequence and its probability. Thus, lower risk estimates for individuals result if larger populations are involved. This problem arises because the degree of exposure to risk is a primary concern, that is, for a measured frequency of occurrence of a consequence from actual data. According to William Rowe (1977), the smaller the group that is exposed to the risk, the higher is the risk to an individual member of the exposed group. Overstatement of the population exposed can lead to understatement of individual risk.

The population at risk must be properly identified for each risk, and it is important to recognize that all members of the population do not necessarily experience the same risk. Thus, the risk rates must often be broken into subsets for different population exposures. The total exposure is properly calculated by integrating the probability of risk for a given individual or group of individuals over the total population. Because the ability to accurately determine the probability for each individual is limited, the resultant calculation may be no more accurate or meaningful than average values taken over subgroups.

Nevertheless, when it is desired to express the degree of containment of risk (i.e., the separation of exposed and protected populations), a degree of containment index may be convenient. This can be computed for any consequence, but to illustrate the concept, we use fatalities. Essentially, the ratio of risk (the relative risk ratio) between the exposed population and the unexposed population is required:

$$\text{Containment index, CI} = \frac{\overline{f_i}}{\overline{f_i'}}$$

where

$\overline{f_i}$ is the risk to an individual in the exposed population

f_i' is the risk to an individual in the protected population

As P_i refers to the exposed population, $T - P_i$ is the protected population, where T is the total population (for purposes of calculating the index, the total T is usually

taken to be the total US or world population; alternatively, P_i is the protected population if the populations considered are not collectively exhaustive). Then

$$\text{CI} = \frac{T - P_i}{P_i} \times \frac{g_i}{g_i'}$$

where

$g_i = N \times F_i$

$g_i' = N_i \times F_i'$

$P_i < T$

$g_i' \leq g_i$

However, this index ranges from unity to infinity, with small changes in factors causing large excursions of the index over parts of the range. A more amenable index is derived by smoothing the range in the form

$$\text{CI} = \frac{T - P_i}{P_i} \times \log \frac{g_i + 1}{g_i' + 1}$$

Alternatively, when multiple populations are involved,

$$\text{CI} = \frac{T - P_i}{P_i} \times \log \frac{g_i + 1}{g_i' + 1}$$

5.4.2 Life Expectancy Models

Baldewicz et al. (1974) developed a model for assessing risk data based on loss of life expectancy. Assuming that all insults (definitions) for a given risk system are linearly independent, the total rate of loss of life, based on 10^6 exposure hours to each stressor, is taken as

$$\dot{L} = 10^6 \sum_i \omega_i \dot{L}_i = 10^6 \sum_i \omega_i \left(\frac{L_i}{T_i} \right)$$

where

$\dot{L} = L_i / T_i$ (loss of life expectancy in years per exposure hour for the ith insult)

L_i is the lost years of life expectancy

T_i is the time of exposure in hours

ω_i is the coefficient of insult intensity

Taking ω_i as unity for fatal insults, it is anticipated that the preponderance of other values of ω_i will lie between 0 and 1. (Possible exceptions are totally immobilizing disabilities or illnesses, for which peripheral insults to family, friends, and society are

involved; or perceived future risks entailing undue, irrational fears). Procedurally, implementation of $\dot{L}$ requires much more information than that typically available for other risk assessment schemes, for instance, treatment of multiple fatalities incurred in a large number of victims, as well as life expectancy data for the calculation of loss of life expectancy due to fatalities L_f for some appropriate actuarial period (taken here to be one calendar year). In general,

$$L_f = \sum_i n_{f,j}\left(A_j - a_j\right)$$

where

n_{fj} is the number of fatalities with age a_i
A_i is the associated life expectancy
N_i is the total number of fatalities
I_f is the average lost years of life expectancy per fatalities for a group at insult during the actual period

Alternatively, $L_f = \Sigma_j n_{f,j}(A_j - a_j)$ can be written as $L_f = N_i(\overline{A_j - a_j}) = N_f I_f$.

These calculations can be made for other types of insult such as property damage expressed in dollars lost: $L_{\text{pd}} = N_{\text{pd}} I_{\text{pd}}$, where N_{pd} is the assessed property damage in, say, dollars, and I_{pd} the "lost years" of life expectancy per assessed dollar of property damage. The latter quantity requires further discussion. To first order, it is assumed that restoration of property simply involves labor (i.e., the intrinsic value of raw materials can be neglected). Furthermore, it seems reasonable to assume that the distribution of labor required in terms of skills and services does not differ appreciably from that residing in the economy at large. Therefore, lost years of life expectancy per assessed dollar of property damage, assuming a 1-year actuarial period, will be taken as $I_{\text{pd}} = (40/168)/I$, where I is the mean income of the nation's labor force and 40/168 is the fractional time employed, assuming a 40-h work week. Problems of interpretation become further complicated when insults assume the form of "deferred" risks. For the special case of a deferred risk that causes premature death, the loss of life expectancy incurred by the population at risk (again, for 1 year actuarial period) will be taken as

$$L_{fd} = \frac{\sum_{a_j}\sum_{t_k} p_r(a_j,t_k) l_{fd}(a_j,t_k)}{P_r}$$

where

a_j and t_k denote admissible ages and cumulative exposure years, respectively, for the subpopulation p_r at risk
P_r denotes the total population at risk $(\Sigma_{a_j}\Sigma_{t_k} P_r(a_j,t_k) l_{fd}(a_j,t_k) = \{\{A_{j+1}t_k + 1)] - [A_j(O) - A_j t_k)]\}$

It must be noted that $l_{fd}(a_j, t_k)$ is to be interpreted as the decrement in mean life expectancy for an individual of age a_j undergoing unit increment in cumulative exposure years from t_k to $t_k + 1$. Similar equations can be constructed for other types of insults, such as morbidity. Based upon this model of Badervicz, w values for l_f, average lost years of life expectancy per fatality, can be calculated; L_f, loss of life expectancy due to fatalities; and N_f, number of fatalities per 10^6 exposure hours for 10 risk systems, making some examination of nonfatal injuries and property damage.

5.5 Fault Tree Analysis

Integrating the statistical likelihood of component events, the fault tree can then be used to estimate the overall probability of occurrence for a desired end result of a failure sequence.

The first step in fault tree construction is selection of the top failure event that is to be the subject of the analysis (McCormick 1981). The next step is to identify contributing events that may directly cause the top event to occur and at least four possibilities that exist (McCormick 1981):

- No input to the device was received, such as signal to operate.
- The device itself has experienced some failure so that it will not operate.
- There is a human error, such as failure to actuate a switch or to properly install the device.
- Some external event may have occurred that prevents operation of the device, such as a common cause failure.

If it is decided that any one of the contributing events can cause the top failure, this occurrence corresponds to the logical OR function of the events (McCormick 1981). Symbols describing the logic of fault tree nodes are unique, but fairly common to engineers and managers (Figure 5.3). The basic symbols in the tree include

- Event symbols—indicating event and status
- Gate symbols—indicating logical relationships between input and output events (AND, NAND, OR, XOR, PRIORITY, NOT, etc.)
- Transfer symbols—mechanisms uniting multiple sections or pages

5.5.1 Example of Event Tree Analysis

Simplified event tree analyses of underground freight transportation and secret WMD fabrication and operation are presented in Figures 5.4 and 5.5, respectively.

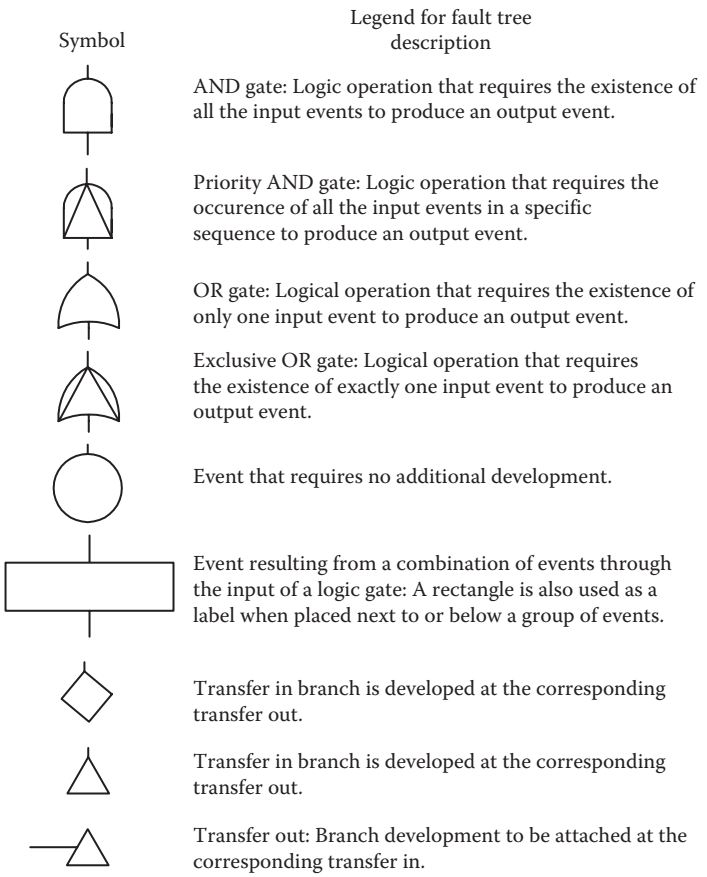


Figure 5.3 Legend for fault tree. (From Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011.)

Probability of successful terrorist attacks on underground freight transportation system:

$$= 0.05 \times 0.80 \times 0.75 \times 0.80 \times 0.60 = 1.4 \times 10^{-2}$$

Probability of unsuccessful terrorist attacks on underground freight transportation system:

$$= 0.95 \times 0.02 \times 0.25 \times 0.20 \times 0.40 = 3.8 \times 10^{-3}$$

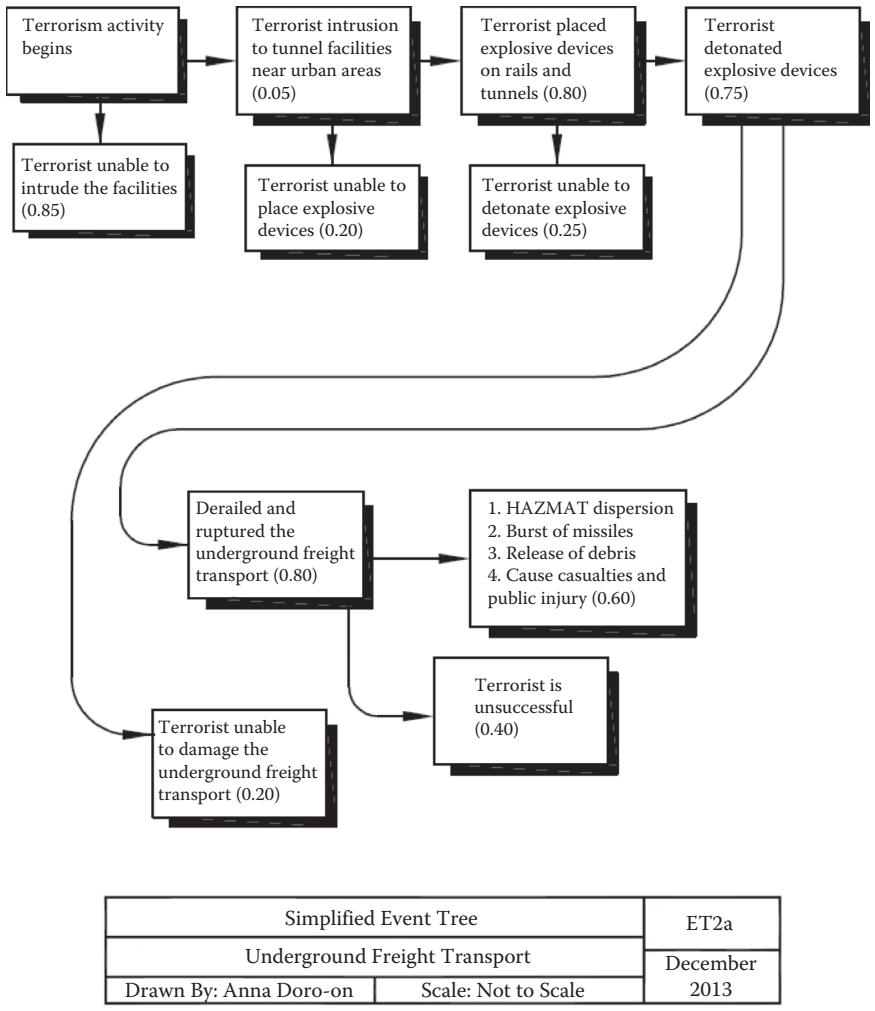


Figure 5.4 Simplified event tree analysis of underground freight transportation terrorism.

Probability of successful WMD development:

$$= 0.095 \times 0.70 \times 0.85 \times 0.50 \times 0.80 \times 0.80 = 1.7 \times 10^{-1}$$

More detailed illustrative examples and presentations of terrorism scenarios, and comparison of event tree analysis to risk acceptability analysis for terrorism and illegal WMD operations in pipeline, rail, and tunnel infrastructure are provided in Chapter 7.

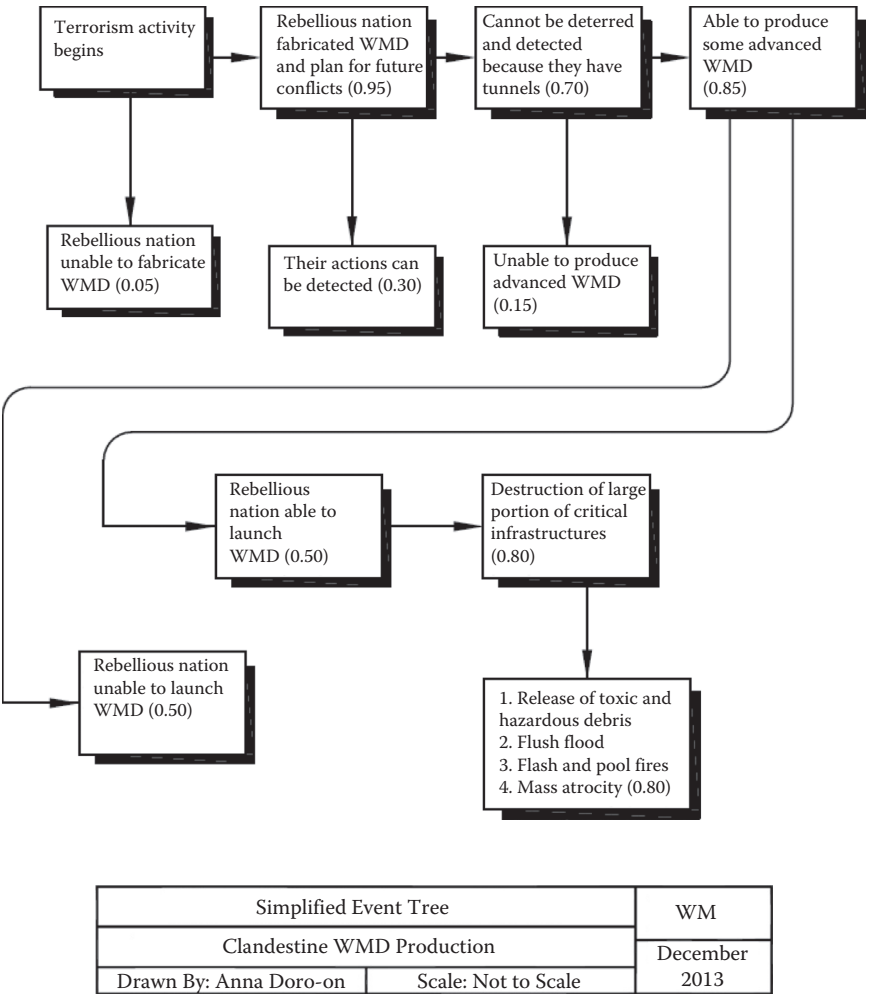


Figure 5.5 Simplified event tree analysis of secret WMD fabrication and operation.

5.6 Identification of Hazards

The identification of terrorism and disaster hazards was derived from data for current freight transportation systems. This method was fundamentally subjective. Available historical data from analogous HAZMAT incident occurrences and severity were important resources for identifying risk for pipelines, tunnels, underground rapid rail, and transit systems. Terrorism can create the following:

1. Misalignment of guideway
2. Track guideway destruction

3. Cyber-controller system failure
4. Operator error
5. Mechanical–electrical equipment failure
6. Flooding short-circuits the guideway
7. Intrusion damages the guideway
8. Explosion within the tunnels entry and exit
9. Flash fire damages the guideway
10. Rupture the maglev train or capsule, or any combination of these damages

The potential economic, environmental, and safety hazards associated with these assets including impacts of clandestine tunnels are identified in Tables 5.4 through 5.7 based on potential events deduction. Pipeline construction, maintenance and operation, rail systems statistics, linear induction motor technology, and historical and experimental freight pipeline system information was used to identify hazards and potential exposure groups.

5.7 Terrorism Intrusion

Illegal intrusion into the secured areas of the pipeline, tunnels, and underground high-speed transport systems is possible via structures designed for operation, maintenance, and repair. Hazards created by unauthorized access might result in vandalism, arson, damage to structural integrity of the tunnel or rail systems, damage to the propulsion system, or burst of infrastructure.

5.8 Flash Fire Probability

Flash fire probability is calculated based on the combined events of hazardous material emission and spill inside freight transportation through pipelines with the condition of an ignition of flammable material caused by a terrorist enemy as illustrated in the fault tree in Figure 5.6. The resultant probability of flash fire by terrorism is 0.01.

Based on the failure probability of key subsystems as shown in Table 5.6, the resultant damage severity of different subsystem by terrorism is summarized in Table 5.8.

5.9 Flash Fire: Ignition of Flammable Materials

The occurrence of fire in the underground rail transport system is much less than that for a ground-level or elevated transportation system. However, as the system

Table 5.4 Summary of the Identified Hazards by Terrorist Attacks on Freight Pipeline Systems

Identified Hazards on Underground Freight Transportation (UFT) through Pipelines	*UFT through Pipeline Damage*	*Environmentally or Security Sensitive Area Damage*	*Public Health Injury*	*Adjacent Critical Infrastructure Damage*
Terrorism intrusion	x	x	x	
Cyber security failure	x			
Security preventive system	x			
Tunnel/ pipeline rupture	x	x	x	x
Adjacent pipeline leak	x	x	x	
Sensor malfunction	x			
Mechanical/ electrical failure	x			
Cyber-controller system failure	x			
Capsule/ freight collision	x			x
Freight damage	x		x	
HAZMAT spill	x	x	x	x
Flash fire	x	x	x	x

Table 5.5 Summary of the Identified Hazards by Terrorist Attacks on Oil and Gas Pipelines

Identified Hazards on Oil and Gas Pipelines	*Oil and Gas Pipeline Damage*	*Environmentally or Security Sensitive Area Damage*	*Public Health Injury*	*Adjacent Critical Infrastructure Damage*
Pipeline fracture	x	x	x	x
Terrorism intrusion	x	x	x	x
Adjacent pipeline leak	x	x	x	x
Sensor malfunction	x			
Security system failure	x			
Mechanical/ electrical failure	x			
Adjacent pipeline explosion	x	x	x	x
Cyber-controller system failure	x			
HAZMAT spill and dispersion	x	x	x	x
Flash fire, pool fire, jet flame	x	x	x	x

Table 5.6 Summary of the Identified Hazards by Terrorist Attacks on Rail and Transit Systems

Identified Hazards on Rail and Transit Systems	*Rail and Transit System Damage*	*Environmentally or Security Sensitive Area Damage*	*Public Health Injury*	*Adjacent Critical Infrastructure Damage*
Terrorist attacks	x	x	x	x
Rail transit rupture and damage	x	x	x	x
Sensor malfunction	x			
Security system failure	x			
Mechanical/ electrical failure	x			
Rail derailment and collision	x	x		
Cyber-controller system failure	x			
HAZMAT and debris dispersion	x	x	x	x
Flash fire	x	x	x	x

is underground and not supplied with free air, the initiation and propagation of a fire would rapidly exhaust intrapipe oxygen. The ignition source can spark from the wheel-on-rail friction or electrical spark from the electrical–mechanical propulsion system. But, a terrorist enemy can increase the chance of having a large impact and change such accidental spark ignition events. All flash fires will be maliciously generated in large scale by the enemy.

5.10 Detonation of Explosive Devices

Placing of explosive devices or human bombs in rail transport systems and oil/gas pipelines is a major concern. Ten explosions rocked through four commuter trains during rush hour on March 11, 2004, in Madrid, Spain and the attack, which was carried out by violent Islamist extremists, killed 191 people, and injured more than 1800 (US Department of Homeland Security 2013). Fifty-two people were killed

Table 5.7 Summary of the Identified Hazards by Clandestine Tunnels and WMD Production by Terror Enemies and Rebellious States

Identified Hazards Generated by Clandestine Tunnels and WMD Production	*Largely Impacts National Security*	*Environmentally or Security Sensitive Area Damage*	*Public Health Injury*	*Adjacent Critical Infrastructure Damage*
During the development and fabrication of WMD				
Terror-military planning and operations in secret infrastructures/tunnels	x			
Manpower mobilization for WMD production through tunnels between nations	x			
Clandestine underground transshipment systems for WMD materials	x			
Illegal intrusions via underground pipelines to homeland	x			
Detection/surveillance system failure	x			
Illegal distribution of explosive devices	x			
Deficiency in international security policy	x			
Successful development of advanced technologies for launching WMD against homeland, allies, and friendly nations	x			
Clandestine underwater or immersed tunnels for security and defense by sly nations and enemies	x			

(*continued*)

Table 5.7 (continued) Summary of the Identified Hazards by Clandestine Tunnels and WMD Production by Terror Enemies and Rebellious States

Identified Hazards Generated by Clandestine Tunnels and WMD Production	*Largely Impacts National Security*	*Environmentally or Security Sensitive Area Damage*	*Public Health Injury*	*Adjacent Critical Infrastructure Damage*
Clandestine construction of underground infrastructures adjacent to high-tech transportation systems and military sites for free flow of manpower mobilization and terror operations by rebellious nations	x			
Successful completion of sophisticated WMD and maturity of terror operations (if illegal secret tunnels and transshipment of WMD materials will not be mitigated)				
Launch of WMD	x	x	x	x
Energy and shock waves release	x	x	x	x
Flash fires, pool fires, and jet flames	x	x	x	x
Preventive systems failure	x	x	x	x
HAZMAT dispersion	x	x	x	x

Immediate emergency response failure (*due to large magnitude of destruction by WMD, most emergency responders and response facilities are destroyed*)	x	x	x	x
Immediate medical response failure (*due to high magnitude of devastation by WMD, most medical facilities and supplies are destroyed*)	x		x	
Immediate shelters and food supplies are unavailable (*due to high magnitude of devastation by WMD, most shelters and food supplies are destroyed*)	x	x	x	
Power and energy supply outage after WMD detonation	x	x	x	x
Water supply outage	x	x	x	x

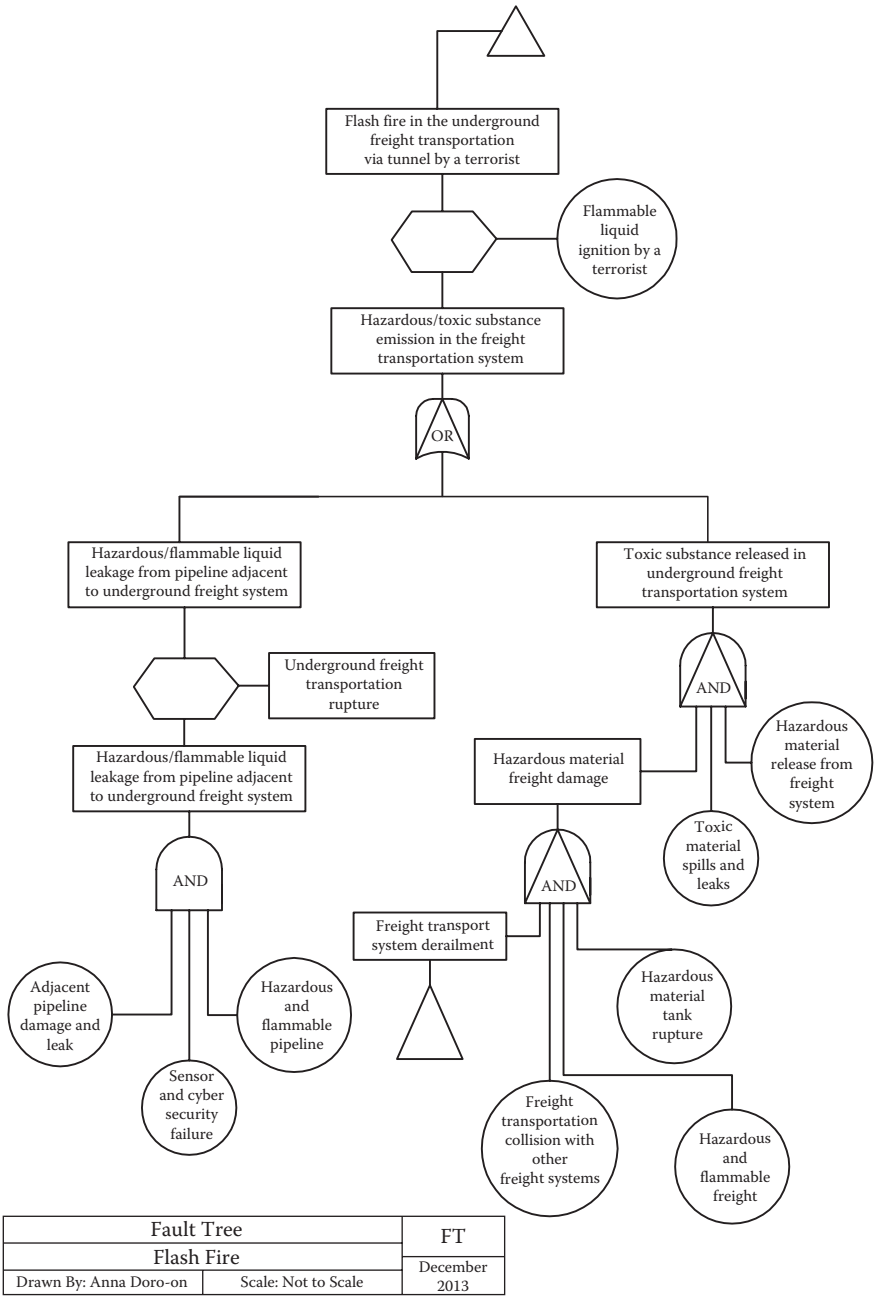


Figure 5.6 Fault tree analysis of underground transportation through pipeline Terrorism.

Table 5.8 Failure Probability of Key Systems and Mechanical Components by Terrorism

Hazard	*Category*	*Failure/Fault Probability*
Terrorism intrusion	Nonroutine	1×10^{-3}
Intruder damages guideway	Nonroutine	3.8×10^{-1}
Contiguous water damage	Condition	9×10^{-2}
HAZMAT in tube freight system	Condition	2.5×10^{-1}
Ignition of flammable material	Condition	3.8×10^{-1}
Electromagnetic damage	Condition	1×10^{-04}
Adjacent to sensitive area	Condition	9.4×10^{-2}
Adjacent to populated area	Condition	1×10^{-2}
Worker exposure to HAZMAT, missiles, fire, and debris	Condition	9.4×10^{-2}
Guideway short circuit	Component	3.8×10^{-1}
Adjacent pipeline leak	Component	4.5×10^{-3}
Sensor failure	Component	4.2×10^{-2}
Mechanical–electrical failure	Component	1×10^{-2}
Derailment of rail and transit system	Component	2.5×10^{-4}
Freight capsule collision	Component	1×10^{-2}
HAZMAT spills	Component	5×10^{-1}
HAZMAT leaks from capsule	Component	5×10^{-1}
Rupture	Component	9×10^{-3}

and hundreds more injured in a series of coordinated attacks on the London transportation system on the morning of July 7, 2005 (US Department of Homeland Security 2013). Moreover, an armed terrorist group detonated with an explosive device a gas pipeline extending from Deir Ezzor to Palmyra (in Syria) and an oil transfer pipeline extending from the al-Omar field to the Atteim field in Murrat village, north of Deir Ezzor (in Syria), causing a fire to erupt at the site (Syrian Arab News Agency 2012). Likewise, armed militants struck an oil pipeline in the southern Yemeni province of Shabwa using rocket-propelled grenades (United Press International Inc. 2012). Though large-scale terrorism against pipelines, tunnels, rail, and transit systems never happened in the United States, the enemies have

never stopped plotting for attacks. One event of a train sabotage happened in 1995 in Palo Verde, Arizona, when Amtrak's Sunset Limited derailed killing 1 person, injuring 78 people, and seriously injuring 12 people.

The probability of terrorism against underground freight through pipelines (i.e., CargoCap, *maglev* trains, and other capsulated freight systems) and rails (i.e., railways and tubular rails) is considerably high. Similar to the 9/11 airplane bombings, fast trains such as *maglev* trains carrying hundreds of people with super high speed typically at 311 mph (500 km/h) can be attacked with WMD to destroy surrounding infrastructures.

5.11 Large-Scale WMD Detonation

Enemies persevere to manufacture chemical, biological, radiological, and nuclear weapons as powerful WMD to intimidate and for potential attacks against homeland, allies, and friendly nations. WMD detonation is the ultimate violent act of terrorism that can diminish a civilization and be used as mass genocide. HAZMAT, violent hazardous particles from explosions, rapid dispersion of poisons, and extreme intensity of heat and shock waves from *WMD attacks can generate mass atrocities approximately in 10 s*. The survivors will likely experience intense pain and suffering that currently no one can imagine. This is a legitimate reason that illegal secret WMD fabrication should be checked by all means.

5.12 Pipelines, Tunnels, Underground Rail, and Transit Systems Adjacent to Human Population

An accidental or malicious release of HAZMAT and collapse of the pipeline system will affect the public. The public is affected due to the contamination of the environment. Other injured human groups include operation and service personnel, construction workers, and third-party workers. Explosions of high-speed rail systems generate mass casualties as the new maglev train usually carries 500–800 people per travel. There is no way to escape in the event of terrorism.

5.13 Guideway Short Circuit

Given that the pipeline/tunnel is subterranean, flash flooding of the freight system or underground rapid transportation system by water could easily result in short circuit of the guideway. There will be portions of the infrastructures where groundwater level is above the tunnel/pipeline invert. Electrical subsystems such as power catenary or linear induction coils are generally vulnerable to water damage.

5.14 Pipelines, Tunnels, Underground Rail, and Transit Systems Adjacent to Critical Assets

Terrorism on pipelines, tunnels, rail, and transit system in overpopulated areas affects not only the surrounding community but also the adjacent critical assets. Burst of missiles, fragments, fireballs, flash fires, and jet flames are all destructive to the surrounding nearest assets.

5.15 Pipelines, Tunnels, Underground Rail, and Transit System Rupture

Loss of integrity of the pipeline due to terrorism causes human injury as well as environmental and safety hazards. If the pipeline or maglev train was damaged by terrorism, a catastrophic explosion could occur, and the contents of the pipeline would be released into the environment or into an urban area.

5.16 Sensor Failure

Sensors are used to detect fires, flooding, toxic release, guideway misalignment, intrusion to secured areas, and pipeline leaks. With the increased sophistication and collateral damage brought on by terrorists, sensor failure could easily increase the likelihood of terrorism success.

5.17 Mechanical and Electrical Failure

Based on the records of rail equipment train accidents attributed to mechanical–electrical failure, the mechanical and electrical failure rate of the freight pipeline system in a protected environment is estimated to be 1% of that of the conventional train system by terrorism.

5.18 Capsules, Underground Rail, and Transit System Derailment and Collision

Given that derailment could occur once per 100 years/500 mile of high-speed ground-level guideway systems, the underground freight transport with capsules travelling through a close-fitting duct with only 1 in. clearance can be derailed by terrorists. The frequency of occurrence of such derailment is estimated to be 0.00020 for each mile per year.

5.19 HAZMAT Freight Container and Pipeline Damage, Collapse, and Spill

Freight is normally protected by a system of quaternary containment in an underground freight transport system and/or CargoCap: the tamper-resistant freight container, the capsule that carries the container, the pipeline concrete shell, and the backfill barrier that covers the tunnel system. Therefore, the likelihood of transport destruction is contingent on failure of the containment system.

The collateral damage is dependent on the hazardous characteristics of the freight. HAZMAT characteristics include ignitability, corrosivity, reactivity, and toxicity. Ignitable materials could ignite and burn or burst into missiles.

5.20 Risk Index Matrix

The risk index matrices given in Tables 5.9 and 5.10 were developed and derived by other experts for pipelines, tunnels, underground rail, and transit systems.

The resultant risk index for each of the consequences does not address the concern of public acceptability at all; it only provides an arbitrary classification.

5.21 Human Injury Risk

The human injury risk based on the fault tree estimated as the human injury created by the combined events of freight pipeline rupture and leaking HAZMAT is approximately as high as 4.0×10^{-5}.

Table 5.9 Risk Index Matrix

	Criticality Infrastructure			
Asset Vulnerability	*Essential*	*Critical*	*Important*	*Not Important*
Extremely high (A)	1A	2A	3A	4A
High (B)	1B	2B	3B	4B
Medium (C)	1C	2C	3C	4C
Low (D)	1D	2D	3D	4D

Note: Risk index numbers 1A, 1C, 2A, 2B, and 3A are considered unacceptable risk. Risk index numbers 1D, 2C, 2D, 3B, and 3C are considered risks demanding management decision. Risk index numbers 3C, 4A, 4B, 4C, and 4B are considered acceptable. Estimated frequencies for different classes of corresponding potential destructions are presented in Table 5.10.

Table 5.10 Severity of Damage versus Risk Index

Severity of Consequences	*Estimated Frequency of Occurrence*	*Risk Score*
Catastrophic damage	0.0091	1A
Critical damage	0.0001	2B
Important damage	0.0095	3A
Negligible damage	0.01	4A

5.22 Implication

Hazards associated with the pipelines, tunnels, and underground transport systems have been illustrated. The frequency of occurrence of each hazard was estimated based on equivalent systems statistics. Fault trees and Boolean logic was utilized to determine the probabilities of the faults. The severity of the consequences and the frequency of occurrence of each fault were determined and the risk index was assigned for each fault. The risks associated with these infrastructures evaluated by using the risk estimation model is found to be more realistic than the risk index method employed by other experts. Currently, we can only identify the vulnerability of assets and their hazards but to be able to implement systematic safeguards and defensive policies, and employ stronger preventive systems, it is critical to measure the levels of acceptable risks. Chapter 6 presents a risk acceptability analysis based on the quantitative psychology of intuitive judgments. More detailed demonstrations of the risk estimation model, probabilistic model, event tree analysis, and risk acceptability analysis are provided in Chapter 7.

References

Baldewicz, W., Haddock, G., Lee, Y., Whitley, R., and Denny, V. 1974. *Historical Perspective on Risk for Large-Scale Technological Systems*. UCLA-ENG-7485. Los Angeles, CA: UCLA School of Engineering and Applied Science.

Bennett, B. 2012. Deterring North Korea from using WMD in future conflicts and crises. http://www.au.af.mil/au/ssq/2012/winter/bennett.pdf (accessed December 2, 2012).

Doro-on, A. 2009. Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX.

Doro-on, A. 2011. *Risk Assessment for Water Infrastructure Safety and Security*. Boca Raton, FL: CRC Press.

Fussell, J. and Arendt, J. 1979. System reliability engineering methodology: A discussion of the state of the art. *Nucl. Saf.* 20:541.

McCormick, N. 1981. *Reliability and Analysis: Methods and Nuclear Power Applications*. London, UK: Academic Press Inc.

Raiffa, H. 1968. *Introductory Lectures on Making Choices under Uncertainty*. Reading, MA: Addison-Wesley.

Rowe, W. 1977. *An Anatomy of Risk*. Toronto, Ontario, Canada: John Wiley & Sons, Inc.

Shih, C. S. 1985. Risk acceptability for handling, analysis and disposal of dioxin in a laboratory. In *Proceedings of the 5th National Conference for the Management of Uncontrolled Hazardous Waste Sites*, Washington, DC. Silver Spring, MD: HMCRI.

Syrian Arab News Agency. 2012. Army inflicts heavy losses upon terrorists in several cities—Armed terrorist group detonates oil and gas pipelines in Deir Ezzor. http://sana.sy/eng/337/2012/10/18/447780.htm (accessed December 31, 2012).

Tribus, M. 1969. *Rational Descriptions, Decisions and Designs*. New York: Pergamon Press.

United Press International Inc. 2012. AQAP tied to Yemeni oil pipeline attack. http://www.upi.com/Business_News/Energy-Resources/2012/04/11/AQAP-tied-to-Yemeni-oil-pipeline-attack/UPI-63271334143652/ (accessed December 3, 2012).

US Department of Homeland Security. 2013. IED attack: What it is. http://www.dhs.gov/ied-attack (accessed February 2, 2013).

Chapter 6

Risk Acceptability Analysis Based on Quantitative Psychology of Intuitive Judgments

6.1 Introduction

Risk acceptability based on *quantitative psychology of intuitive judgments* is necessary in homeland and critical infrastructure protection against terrorism and disaster. It is involved with the measurement of the degree of risk that can be accepted by stakeholders and society for given risk events. Risk acceptability can be understood by asking these questions: *How safe is safe enough? Which levels of risk are acceptable? How to maintain intuitive judgments in determination of acceptable risks? What specific risk situations are permitted? Acceptable to whom?* It is the objective of this chapter to provide a clear demonstration of a quantitative approach to risk acceptability embedded with a *cumulative prospect theory* and to address these five questions in relation to pipelines, subterranean infrastructures, tunnels, rail, and transit systems security and *intuitive* recognitions or predictions of illegal secret production and distribution of weapons of mass destruction (WMD).

6.1.1 Public Perception of Risk: Quantitative Psychology of Intuitive Judgment and Cumulative Prospect Theory

Risk perception is the perceived judgment by an individual, group of people, or society about the attributes, condition, and severity of a risk. Decision makers and risk analysts do not always react with perfect rationality to prospects of loss and gain in the presence of risk because individual perception impacts decisions. If every individual perceived the world around him or her in the same manner, there would be no difficulty in assessing the acceptability of a particular risk situation or event (Doro-on 2011). In the real world, people often fail to predict reality very clearly. Risk issues occur in different cases, in which experts and authors are often interested, but none is completely organized and finely documented. They are often surrounded by a large degree of uncertainty resulting from such diverse causes as limited knowledge and restricted measurement capabilities (Doro-on 2011). Compounding these limitations is the complexity of the problem, not just based on the multiplicity of risk pathways but also because risk does not exist by itself (Doro-on 2011). It is only one of many problems that must be considered as simply one factor in a morass of benefits and costs, which can be direct and indirect, that surround any public decision problem (Doro-on 2011).

Uncertainty is an unavoidable aspect of the human condition (Tversky and Kahneman 1983). Many significant choices must be based on beliefs about the likelihood of such uncertain events as the guilt of a defendant, the result of an election, the future value of the dollar (Tversky and Kahneman 1983), or an action in the event of terrorist attacks. Because we normally do not have adequate formal models for calculating the probabilities of such events, *intuitive judgment* is often the only practical method for assessing uncertainty (Tversky and Kahneman 1983). The psychology of judgment to the evaluation of legal evidence needs careful study because the outcomes of many trials depend on the ability of a judge or a jury to make intuitive judgments on the basis of partial and fallible data (Rubinstein 1979, Saks and Kidd 1981). Likewise, judgment to the detection of terrorism activities and developing scenarios requires extensive analysis. The development of terrorism and disaster scenarios is often used in the framework of planning, and the integrity of these scenarios influences significant decisions in terms of security and defense. Tversky and Kahneman's (1983) analysis suggests that *a scenario that includes a possible cause and outcome could appear more probable* than the outcome on its own.

The judgments and decisions that we are most likely to call intuitive come to mind on their own, without explicit awareness and of course without an explicit evaluation of the validity of these cues (Kahneman and Klein 2009). Intuitions that are available to a few exceptional individuals (*talent surely matters*) are often called *creative*; however, *creative intuitions* are based on finding valid patterns in memory, a task that some people perform much better than others (Kahneman and Klein 2009). When intuitive judgments do not come from the skill of those that

are considered imperfect intuitions, where then do they come from? The answer is that they result from the following situations (based on the study of Kahneman and Klein [2009]): (a) decisions based on gut feelings and intuitions that are not precisely evaluated; (b) the anchoring phenomenon is another case in which a bias in the operations of memory causes intuitions to go astray; (c) immediate intuitive impression, when that single response comes to mind. The recognition model implies that two conditions should be satisfied for an intuitive judgment to be genuinely skilled: (a) the environment must provide adequately valid cues to the nature of the situation; (b) people must have an opportunity to learn the relevant cues (Kahneman and Klein 2009).

Intuitive judgments in homeland and infrastructure security and defense require the following:

1. Talent in intuitive judgments
2. Environment where you can exercise that talent with regularities
3. Opportunity of learning and acquiring training to maintain intuitive recognitions or judgments

A potential imperfection of intuitions can likely occur when any of these attributes do not exist. Real expertise in prediction of clandestine subterranean infrastructures (i.e., production of WMD), secret and illegal transport of WMD, and terrorism and disasters requires the following: engineering knowledge of these infrastructures, practical experience, extensive practice and learning processes, so that expert intuitions can be accurate. Mostly, experts rely so much on available technologies but that could limit their judgments without having authentic creative skills in intuitions. They could be confident with their ego due to their many years of experience, but they may not have been able to develop their intuitive skills.

The critical question that Kahneman (2011a) pointed out is: *When can you trust a self-confident professional who claims to have an intuition?* People's confidence rests in a belief of two related impressions: cognitive ease and coherence, so we are confident when the story we tell ourselves comes easily to mind, with no contradiction and no competing scenario (Kahneman 2011a). The confidence that people have in their intuitions is not a reliable guide to their validity, and do not trust anyone including yourself to tell you how much you should trust their judgment (Kahneman 2011a). *There has also been a fair amount of research indicating there are classes of decision where following your gut is a good idea* (Kahneman 2011b). *It's much more limited than most people think* (Kahneman 2011b). We're very inclined to take subjective confidence at face value, that is, to assume that if an individual feels confident in a judgment or in a decision, then that must be valid (Kahneman 2011b). People are extremely confident even when they don't know what they are talking about or don't know what they are doing (Kahneman 2012).

> If subjective confidence cannot be trusted, how can we evaluate the probable validity of an intuitive judgment? When do judgments reflect true expertise? To distinguish intuitive thoughts that you can trust from those you can't trust you really have to look at the environment and you have to look at the individual's opportunity to learn the environment. (Kahneman 2011b)

According to Kahneman (2011b), confidence is a mark of intuitive thinking regardless of whether intuitive thinking is expert intuitive thinking or heuristic intuitive thinking. So you have to look at the world, and not at people's confidence (Kahneman 2011b).

Moreover, Kahneman and Tversky began all their investigations with thought experiments that they used to probe their own intuitions about statistical matters, but they followed good scientific practice in following them up with rigorous real experiments that showed that many other people had the same erroneous intuitions (Thagard 2012). Great scientists like Galileo and Einstein undoubtedly used thought experiments to advance their research, but acceptance of their ideas depended on the accumulation of experimental results arising from careful observations of interactions with the world (Thagard 2012). Philosophers should follow scientists in restricting their use of thought experiments to the generation and clarification of hypotheses, and to the demonstration of inconsistencies in rival hypotheses (Thagard 2012). Real experiments produce evidence that is repeatable and robust in that it can be obtained by different people in different ways through interaction with the world (Thagard 2012).

Nobel laureate Daniel Kahneman and Amos Tversky had three aspects of research related to intuitive judgment and decision making. The first explored the heuristics that people use and the biases to which they are prone in various tasks of judgment under uncertainty, including predictions and evaluations of evidence (Kahneman and Tversky 1973, Tversky and Kahneman 1974, Kahneman et al. 1982). The second was concerned with prospect theory, a model of choice under risk (Kahneman and Tversky 1979, Tversky and Kahneman 1992) and with loss aversion in riskless choice (Kahneman et al. 1990, 1991, Tversky and Kahneman 1991). The third line of research dealt with framing effects and with their implications for rational-agent models (Tversky and Kahneman 1981, 1986). Psychology offers integrative concepts and midlevel generalizations, which gain credibility from their ability to explain ostensibly different phenomena in diverse domains (Kahneman 2003). A unified treatment of intuitive judgment and choice, which builds on an earlier study of the relationship between preferences and attitudes (Kahneman et al. 1999) and extends a model of judgment heuristics, was proposed by Kahneman and Frederick (2002). *Judgments* are always explicit and intentional, whether or not they are overtly expressed (Kahneman 2003). *The guiding ideas are: (a) that most judgments and most choices are made intuitively; and (b) that the rules that govern intuition are generally similar to the rules of perception* (Kahneman 2003).

There is substantial agreement on the characteristics that distinguish the two types of cognitive processes, for which Stanovich and West (2000) proposed the neutral labels of Intuition (System 1) and Reasoning (System 2). The operations of Intuition (System 1) are fast, automatic, effortless, associative, and often emotionally charged; they are also governed by habit, and are therefore difficult to control or modify (Kahneman 2003). The operations of Reasoning (System 2) are slower, serial, effortful, and deliberately controlled; they are also relatively flexible and potentially rule-governed (Kahneman 2003). The technical term for the ease with which mental contents come to mind is *accessibility* (Higgins 1996). To understand intuition, we must understand why some thoughts are accessible and others not (Kahneman 2003). Findings about the role of optimism in risk taking, the effects of emotion on decision weights, the role of fear in predictions of harm, and the role of liking and disliking in factual predictions—all indicate that the traditional separation between belief and preference in analyses of decision making is psychologically unrealistic (Kahneman 2003).

Tversky and Kahneman formulated prospect theory when they studied and did numerous experiments on *risky choice*. Prospect theory describes decisions between alternatives that involve risk, explicitly alternatives with uncertain outcomes, where the probabilities are given. It explains the major violations of expected utility theory in choices between prospects with a small number of outcomes (Tversky and Kahneman 1986). There are two key elements of prospect theory (Tversky and Kahneman 1992):

- The value function of prospect theory is steeper for losses than for gains.
- There is a nonlinear transformation of the probability scale in prospect theory, which inflates small probabilities and deflates moderate and high probabilities.

That is why people are interested not only in the benefit they receive but also in the benefit received by others. This hypothesis is consistent with psychological research into happiness, which finds that subjective measures of well-being are relatively stable over time, even in the face of large improvements in the standard of living (Easterlin 1974, Frank 1997). Kahneman and Tversky (1979) tested this implication and found that subjects systematically preferred to accept risk when prospects were presented in terms of costs and avoidance of risk than when the same prospects were presented in beneficial terms. Thus, Kahneman and Tversky remodeled prospect theory and presented in 1992 a theory that gives rise to different evaluations of gains and losses, which are not distinguished in the standard cumulative model, and that provides a unified treatment of both risk and uncertainty.

The modification is made, as in rank-dependent expected utility theory, and cumulative probabilities rather than the probabilities themselves are transformed. This brings us to the aforementioned inflating of extreme events (e.g., terrorism against freight of nuclear weapon materials), which occur with less

likelihood, rather than a deflating of all less likely occurrences. The adjustment and variant of prospect theory helps to prevent a violation of first-order stochastic dominance and makes an attainable generalization to arbitrary outcome distributions (Doro-on 2011).

Kahneman and Tversky (2000) concluded that the intuitive and cognitive abilities of a normal human being are clearly overwhelmed by this complexity, thereby forcing him or her to rely on simplified and standardized rules of thumb. These reduced decision-making rules always create bias and imperfect judgments. For instance, one such heuristic as judging the probability of a risk based on the contentment which can be delivered to the public's mind can clearly direct to biases. This heuristic at least partially accounts for the media's capability to mislead or distort the public's perception of risk (Doro-on 2011). Under these situations, it is often complex to evaluate the public's acceptability of an assigned risk.

An anatomy of human perception and its influence on discretion behavior based on experimental evidence is generalized in cumulative prospect theory (Doro-on 2011). Based on cumulative prospect theory, one can no more utilize the anticipated values (i.e., probability and consequence) to describe the preference ordering of choices (Doro-on 2011). Instead, one must also incorporate functions that account for the differences in perception due to the different ways in which problems are framed (i.e., the observer's conception of the problem, consequences, and contingencies) (Doro-on 2011). Therefore, instead of the generalized expected value of risk, one gets (Doro-on 2011)

$$\begin{aligned} V(f) &= V\left(f^{+}\right) + V\left(f^{-}\right) \\ V\left(f^{+}\right) &= 0\left(\text{no gain for terrorists attack}\right) \end{aligned} \tag{6.1}$$

Therefore,

$$\begin{aligned} V(f) &= V\left(f^{-}\right) \\ V(f) &= \omega(p)v(x) \end{aligned} \tag{6.2}$$

where

$\omega(p)$ is the decision weight associated with the probability of occurrence
$v(x)$ are the values associated with consequences
$V(f)$ is the risk

This theory is a mechanism to construct and develop the quantitative psychology of intuitive judgments involved in the development of perception. Hypothetical value and decision weight functions derived from Kahneman and Tversky (2000) are depicted in Figure 6.1. If $\omega(p)$ and $v(x)$ were linear throughout, an expert or a decision maker's intuition or decision would be exclusive of the problem's framing.

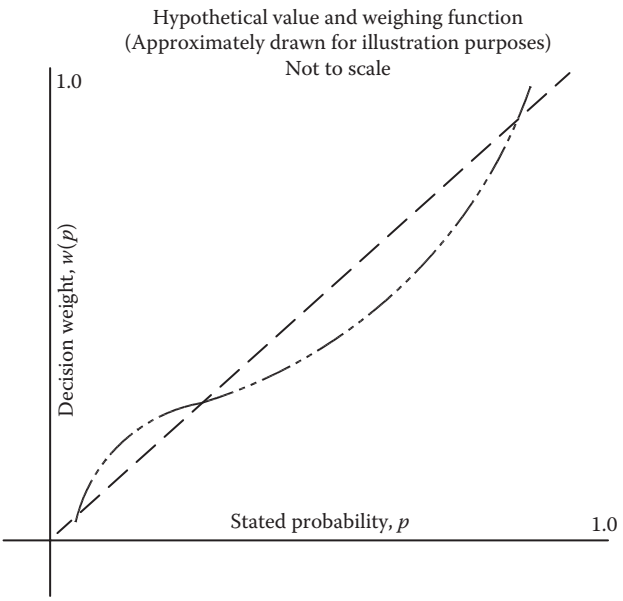


Figure 6.1 Hypothetical probability function. (Derived from Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011; Doro-on, A., Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX, 2009; Shih, C.S. et al., *Risk Assessment of Terrorism Based on Prospect Theory for Groundwater Protection. Vol. 1, Environmental Science and Technology*, American Science Press, Houston, TX, 2007; Kahneman, D. and Tversky, A., *Choices, Values and Frames*, Russell Sage Foundation, New York, 2000.)

Thus, different frames can lead to different judgments and decisions as a result of characteristic nonlinearities while the predicted results of choices stay the same. Some of the most complete analyses, at least for the specific area of intuitive risk assessments, are presented in Sections 6.1.1.1 through 6.1.1.8.

6.1.1.1 Voluntary or Involuntary

Perception seems to be clearly affected by whether a risk is incurred by one's decision or not. For example, one usually expects an engineer facilitating a prolonged site cleanup in the vicinity of radioactive/hazardous waste or a worker inside a vinyl chloride plant to be much more tolerant to risk than the neighboring people. People also are exposed to hazards that are beyond their control, as the risks are involuntary and do not arise from a willful decision (Callan and Thomas 2010). A characteristic of involuntary risk is that individual responses are limited (Callan and Thomas 2010).

6.1.1.2 Discounting Time

An event currently happening tends to be valued higher than the same event occurring at some time in the past. This corresponds with the long-held financial concept that a dollar in the past is worth more than the same dollar today according to an inflationary perspective of the world. Time discounting is the phenomenon that a desired result in the future is perceived as less valuable than the same result now. Economic theories can take this psychological fact into account in several ways (Dimitri and van Eijck 2012). The length of time one is subjected to a risk also seems to affect the valuation process in the form of discounting risk (Nogami and Streufort 1973). The notion that the subjective perception of time is more contracted than objective time has deep roots in Western philosophy and the psychology of time (Sherover 1975, Fraisse 1984, Fredrickson and Kahneman 1993, Read and Loewenstein 1995, Turetzky 1998). Most people are averse to short delays in gratification now, while their future selves may not mind a bit of extra waiting (Dimitri and van Eijck 2012). This behavior can be described well by nonexponential discounting functions such as *hyperbolic discounting* (Dimitri and van Eijck 2012). In hyperbolic discounting, valuations fall rapidly for small delay periods, but the fall gets slower for longer delay periods and captures phenomena such as procrastination, addiction, and, in general, inconsistency over time (Dimitri and van Eijck 2012).

6.1.1.3 Identifiability of Taking a Statistical Risk

Whether a risk will be taken by or imposed on individuals or a society with which one identifies or in which one is just a "number in the crowd" influences an individual's perception of risk. A classic example of this can be seen in the expending of huge amounts of money to rescue trapped miners who have become identifiable while begrudging support to routine safety budgets. Known circumstances and conditions are more highly valued than hypothetical ones.

6.1.1.4 Controllability

People appear to accept higher risk when they feel comfortable that the situation is well under control such as when they are driving an automobile. On the other hand, there is the capacity to control risks that reach acceptable levels by technological and institutional processes in terms of man-originated risks such as terrorist attacks. However, it is not always applicable to risks resulting from acts of God (natural disasters) because the public tends to accept higher risks from natural disasters. Hence, in combating improvised explosive devices (IEDs), risk can only be controlled by using intelligent devices such as systemic controls and enforcing regulatory requirements for the employment of these devices as institutional processes (this topic will be discussed further in the following chapters) for the

protection of pipelines, rails, transit, and tunnels. The controllability factor for illegal secret production of WMD is to intuitively identify the features of these secret infrastructures and mitigate the adversaries by acquiring some technologies that can aid their operations by strategic systemic controls. Further discussions are presented in Section 6.3.3.

6.1.1.5 Avoidability of Risks

Natural disaster risks can be *avoidable*, as a person or a society can change their exposure to possible risks and minimize the likelihood of being affected from hazard or catastrophe. An individual, a group of people, or a society has the ability to recognize danger and choose their location or find an area with lesser likelihood of disaster. The degree of avoidability depends on some natural and man-made disasters. For instance, one can choose to construct a residential structure away from a flood path area or during a storm event, or a society can be relocated in a safer aboveground vicinity to mitigate calamity. There are absolutely unavoidable risks, which are beyond the control of man and fall under the acts of God (e.g., tsunami and high-magnitude earthquakes of March 11, 2011 in Japan). The concerns regarding whether terrorism can be avoided or not depend on the degree of controllability of risks. The exposure to such hazards can be reduced by the employment of layered systemic controls. Intuitive predictions to illegal distribution of WMDs and terrorist operations surely can lead to early prevention of successful large terror attacks. Adversaries and rebellious societies or nations do not usually follow rules and regulations imposed on them. The only way to hinder them from acquiring illegal basic weapons or WMDs is to use other means.

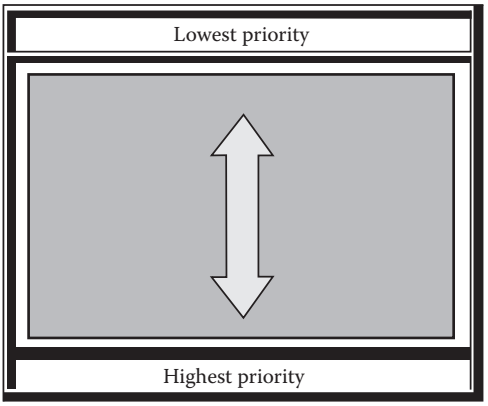
6.1.1.6 Position in Hierarchy of Consequence

The desire to prevent an unwanted consequence depends heavily on the perceived undesirability, that is, position in a desirable–undesirable hierarchy, of the consequence as shown in Table 6.1. As a result, once would normally expect the threshold for acknowledging risk to be much lower for fatal or catastrophic situations than for ones involving risk to security.

6.1.1.7 Ordinary or Catastrophic

A large number of fatalities happening in a single accident have greater impact than the equivalent number of fatalities spread randomly over a number of smaller accidents within the same period. For instance, a greater risk tolerance is expressed by the public for automobile accidents (which are normally ordinary) versus commercial aviation accidents (which tend to be catastrophic).

Table 6.1 Consequence Hierarchy

Lowest Priority	*Self-Actualization*
	Egocentric
	Belonging/love
	Security
	Exhaustible resources
	Security
	Exhaustible resources
	Survival factors
	Illness and disability
Highest priority	Death

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011; Doro-on, A., Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX, 2009.

6.1.1.8 Natural or Man-Originated

Risks imposed by natural disasters such as storms, earthquakes, or volcanic eruptions tends to be much more acceptable than man-originated risks (e.g., terrorism) probably because man has always considered that natural disasters are attributed to acts of God. Potential man-originated risks have been the primary concern in recent years due to the current threats of North Korean, Iranian, and other nations' WMD and terrorists' IEDs against homeland and critical infrastructures. The launch of the North Korean satellite into orbit on December 12, 2012 increased the concern of security risk.

6.1.1.9 Magnitude of Probability of Occurrence

The perceptions of a consequence are not continuously influenced by the degree of the probability of that consequence. This often results in very small probabilities being inflated and the level of risks acceptable to an individual or group can be expected to vary. As a result, we see situations such as the nuclear power plant controversy on acceptability of a risk event.

If an individual desires to use subjective perceptions in his or her assessments, then risk must be distinguished into categories that correspond with the variations between reality (or one's best discretion) and these perceptions.

6.2 Strategic Determination of Risk Acceptability

A number of possible strategies for addressing the questions "How safe is safe enough?" and "Which risks are acceptable?" have been proposed. Three basic approaches can be readily identified: The first is the formal analysis approach. The principal methods included in this category are cost-benefit analysis and decision analysis. This approach relies heavily on formal logic and optimization principles. Meanwhile, *cost–benefit analysis* involves the analysis of cost effectiveness of risk reduction, while *benefit–cost analysis* is involved when risk is a surrogate for social cost.

The next technique is the comparative analysis approach, which is composed of three distinct methods: (1) revealed preference, (2) expressed preference, and (3) natural standards. In this approach, an absolute acceptable risk boundary is developed against which the estimated risk can be evaluated. The last crucial category is professional judgment (e.g., scientific and engineering judgment). This relies principally on the perceptive intelligence and experience of the professional individual or group. A detailed comparison of each approach utilizing five key characteristics—decision-making criteria, locus of wisdom, principal assumptions, possible decision attributes, and data requirements—is given in Table 6.2. Each of these techniques has strengths and weaknesses (Table 6.3). Cost-benefit is very limited, as any element that cannot be transformed to economic terms is disregarded. The formal analysis methods, particularly the decision analysis, impart structure assessment. Both formal techniques, cost-benefit and decision analysis, require large amounts of detailed and reliable data and information of failure to entrench public subjective perceptions of risk into the equation.

All the comparative analysis methodologies have the advantage of determining *absolute* risk boundaries. All three techniques are only intended to address risk and they are incapable of handling the overall decision problem. Furthermore, both revealed and expressed preference methods depend on the limitations of society and its citizens.

6.3 Quantitative Revealed Societal Preference Method

The quantitative revealed societal preference method identifies and synthesizes existing databases relative to societal risk before using these data to calculate the relative impact of risk factors as risk referents for use in risk acceptability analysis. According to Rowe (1977), two aspects of risk valuation are addressed: (1) relative risk and (2) absolute risk. Relative risk provides an initial screening of the effect of risk factors or risk rates on risk valuation through the comparison of different risks, whereas absolute risk represents an effort to evaluate, analyze, and differentiate quantitatively the risk acceptance levels for all types of risk based on revealed societal preference. Meanwhile, accidental risks (e.g., nuclear

Table 6.2 Comparison of Techniques

Techniques	*Decision Making*				*Data Requirement*
Formal Analysis	*Criteria*	*Locus of Wisdom*	*Principal Assumption*	*Decision Attributes*	*Possible*
Cost-benefit analysis	Most favorable economic condition	Standardized intellectual procedure	Man should be a rational economic maximizer; decision is entirely objective	Anything that can be materialized to money	All significant events, conditions, and consequences related to money or wealth; precise probabilities and risk magnitudes for each
Decision analysis	Utility optimization	Formalized intellectual processes	Man is or should be a rational utility maximizer; decision should utilize the decision makers' value (professional) judgments	Any value	All significant events, conditions, and consequences related to money or wealth; precise probabilities and risk magnitudes for each
Revealed preference	Preservation of historical stability	Decisions were made historically by the society	Decisions made historically by society were optimal; little or no change in the events	Risk only	Present risk; historical risk

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011; Doro-on, A., Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX, 2009.

Table 6.3 Techniques' Strengths and Weaknesses

Techniques of Formal Analysis	*Strengths*	*Weaknesses*
Cost-benefit analysis	Logical approach Easy to perform analysis Deal with all types of decision aspects	Discounts attributes that cannot be easily transformed to economic terms and conditions Requires ample detailed data and/or information Difficulty to process subjective value judgments
Decision analysis	Logical approach Easy to perform analysis Compliant or adaptable Deals with all types of decision aspects Incorporates decision maker's (professional) judgment Handles uncertainty	Requires ample detailed data and/or information Cannot deal with public perceptions of risk
Revealed preference	Establishes absolute boundaries Incorporates historical experience and event	Historical decisions often were not always optimal Situations and events change rapidly with time Disaggregated historical baseline hard to establish Does not address the entire decision subject to inherent limitations of society and its citizens

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011; Doro-on, A., Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX, 2009.

power accidents) provide the most straightforward database, which can be used as a comparison to risks related to terrorist attacks, as there are no standard risk factors associated to terrorist attacks.

6.3.1 Behavior and Risk Attitude

Revealed societal preferences are used to generate a risk referent according to the typical notion that that the societal behavior is acceptable no matter whether it is right or wrong. Harry Otway (1975) pronounced the use of existing societal behavior of this nature in the method of revealed societal preferences, which involves the psychological and psychometric study of behavior in identified groups or strata of society, and attempts to measure attitudes toward risk as opposed to risk behavior.

6.3.2 Establishing Risk Comparison Factors

Risk comparison factors can be determined for different types of consequences and risks. Risk data are given for fatalities, illnesses, property damage, life-shortening factors, and productive days lost, by some government agencies such as the US Census Bureau (USCB) or US Environmental Protection Agency (USEPA), which can be analyzed and quantified. Nevertheless, there are not enough available risk data for terrorism; therefore, data of fatal automobile accidents and/or nuclear power accidents will be utilized for the risk analysis of terrorist attacks on groundwater and the water supply system in the United States. There should be some data available in intelligence and military operations as discussed in Chapter 7. But for academic purposes, the risk references presented in this book are valid enough to be used in Chapter 7 for intelligence analysis and military operation decision-making examples. Consequently, the magnitude of fear and consequences created by nuclear power accidents is comparable to that of terrorism. Additional data involve consequences of types that are less agreeable to objective standards, such as esthetic values and quality of life. The USEPA actually listed four major life factors (US Environmental Protection Agency 1973, 2009): (1) household and environmental economic condition (e.g., adequate income and job opportunities), (2) health (e.g., safety and environmental sustainability), (3) natural resources and amenities, and (4) vibrant community (e.g., attracts businesses and retirees). It is evident that humans accept different levels of risk for different types of risk (e.g., voluntary risk versus involuntary risk) (Velimirovic 1975). Refer to Chapter 5, Sections 5.4 and 5.4.1 for risk conversion factors.

6.3.3 Controllability of Risks

Controlling risk based on one's perception of controllability as an individual or group and the *degree of systemic control* provided by regulatory requirements, as

well as technological and institutional processes can potentially increase the value of consequences and risk acceptability. Technological innovations to improve security from terrorism and disaster reduce environmental and societal hazard, prevent production or illegal transit of WMDs, and accidental mishaps are commonplace. On the other hand, society is becoming increasingly aware of and focused on the requirement that sophisticated technology be used to protect the entire population. Therefore, terrorist attacks on pipelines, rails, and tunnels and illegal access to nuclear bomb materials can be mitigated when new intelligent sophisticated technology for security and surveillance is implemented. Reduction of risk is in itself considered to be a benefit. Three main classes of benefit are as follows: (1) materialistic (economic survival), (2) physical protection and security (e.g., protection against terrorist attacks), and (3) self-advancement (free from chaos and distress).

6.3.4 Perceived Degree of Control

The perceived *degree of control* (as opposed to the "real degree of control") to avoid a risk consequence by a valuing factor is a primary condition in defining consequence value. The degree of controllability, whether real or perceived, must be crucially considered.

6.3.5 System Control in Risk Reduction

A society concerned about exposure to risks from new or ongoing activities of humans or from natural causes can achieve the reduction of risk systematically. For example, flood control projects by the Federal Emergency Management Agency (FEMA) saves many lives from naturally occurring flood conditions. Illegal manufacturing WMDs and destruction of infrastructures by terrorists or rebellious societies can be prevented if security technology is implemented and other preventive actions are taken.

6.3.5.1 Systemic Control of Risk

More formally, systemic control of risk as presented in Table 6.4 requires a standard procedure that must be implemented to control risks which includes the following:

- A standard measure of controlling and reducing risk that is given the most emphasis in the design and operation of the technological system involved
- A regulatory requirement or policy of the overall system to assure maximum safety and security
- A system design that includes the following: quality control, redundancy for critical systems, training and educating personnel involved, and ongoing screening of system performance to meet enforcement and auditing system goals in accordance with the regulatory or policy requirements

Table 6.4 Systemic Control of Risk

Positive	*Level*	*Negative*
Systemic control of risk		
1. Risk must be balanced with lesser value to ensure that the risk per unit of measure of technological system performance and operation is decreasing over time.	1. Risks increase over time no faster than the technological system's rate of development, either absolutely or relatively. Or risks maintain the same value over time.	1. When systemic control concept is not considered and/or a technological system whose risk behavior is characterized by an increase in risk over time.
2. Technological systems that are designed and built with positive systemic control as a goal (e.g., weapons and defense system).	2. Whose risk behavior is described by an equilibrium level of risk over time.	

Other types of control		
Control through Specific Design Features	*Control by Inspection and Regulation*	*Risk Management System*
Safety is achieved through special and specific design features of the technological system that provide safety and security (e.g., the use of alternate reverse osmosis system to remove prescription drugs in the water supply is an example of specific design featured to reduce risk).	Positive control is to be achieved, not through special and specific designs, but through inspection and regulatory requirements for the technological systems (e.g., recall of defective Toyota Yaris automobiles in the United States that occurred between 2009 and 2010 is an example of proposed positive control). Regardless of whether it is combined with specific design features, control by inspection and regulation is part of reducing risk in high-risk situations.	Combine control through special design features of the technological system involving inspection and regulation. It is a crucial measurement of achieving systemic control.

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011; Doro-on, A., Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX, 2009; Rowe, W., *An Anatomy of Risk,* John Wiley & Sons, Toronto, Ontario, Canada, 1977.

6.3.5.2 Control Factors

The four control factors required to give a degree of controllability value for every combination are as follows: (1) control approach, (2) degree of control, (3) state of implementation, and (4) basis for control effectiveness.

6.3.6 Controllability of New Technological Systems

Controllability of new technological systems indicates the requirement for practice of a systemic control of risk. As no data are established to evaluate controllability, the effective calculated different levels of controls are based entirely on judgment of value—in this case, the author's engineering discretion.

The level of desirability of control is defined as

$$F3 = C_1 \times C_2 \times C_3 \times C_4 \tag{6.3}$$

where

$F3$ is the condition for a given risk with controls (minimum of 0.01 and maximum of 1.0)
C_1 represents no control
C_2 represents uncontrolled
C_3 and C_4 are ignored (set at unity)

6.3.7 Cost–Benefit Analysis

A cost–benefit (loss–gain) analysis consists of two processes: (a) first, an overall comparability of gains and losses; and (b) second, a specific analysis to determine whether inequities have been improved. Wilson (1975) presented a four-process analysis: (a) we must be sure we understand the benefit and the risk and that the former outweigh the latter; (b) we must be sure we have chosen the method of achieving benefit with the least risk; (c) we must be sure we are spending enough money to reduce the risk further; and (d) we must go back and recheck our numbers with a new perspective from the preliminary calculations.

Rowe's (1977) technique is composed of four principal steps: (1) design an applicable risk classification scheme; (2) define an absolute risk reference for each category in the scheme; (3) using risk references as a basis, quantify the risk reference that performs as the acceptability boundary for particular conditions; and (4) examine and balance the estimated risk within an order of magnitude of the reference to be acceptable. As indicated in Table 6.5, these processes explicitly include the objective to subjective transformation factors. Risk assessments must be divided into different parts to understand the aspects that direct to subjective perception.

The fundamental classification scheme advocated by Rowe (1977) is perception and is shown in Table 6.6. In addition, the hierarchy of consequences as shown in Table 6.1 illustrates that the value of a consequence is associated to life and health.

Table 6.5 Transformation Factor Utilization in Risk Referents

Factors that are unequivocally integrated in the absolute risk reference determination:
Voluntary or involuntary
Discounting of time
Identifiable statistical risk taker
Position in hierarchy of consequences
Ordinary or catastrophic
Natural or human-originated
Factors that are unequivocally integrated in the determination of a risk referent:
Controllability
Propensity for risk taking
Other factors:
Magnitude of probability of occurrence

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011; Doro-on, A., Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX, 2009; Shih, C. and Riojas, A., Risk and its acceptability for groundwater contamination by hazardous wastes, in *Risk Assessment for Groundwater Pollution Control*, W. McTernan and E. Kaplan, eds., American Society of Civil Engineers (ASCE), Reston, VA, 1990, pp. 126–157; Rowe, W., *An Anatomy of Risk*, John Wiley & Sons, Toronto, Ontario, Canada, 1977.

Once a classification scheme is applied, an absolute risk reference must be determined and defined for every category. These are approximated from historic societal risk data as *revealed preferences*. The risk references derived from the data provided by Rowe (1977) for immediate statistical accidents are shown in Table 6.7. In practical applications in the real world, one must check if latest data are available; especially a military operation should have ample recent data that can be developed and used for intelligence and military operations as presented in Chapter 7.

For the risk $V(f)$, defined by Kahneman and Tversky's cumulative prospect theory, risk reference is essentially the value of consequence, $v(x)$ (Doro-on 2009, 2011). Using the revealed preference concepts, the $v(x)$ or risk reference is really the currently acceptable risk by the US society as shown in Figure 6.2 (Doro-on 2009, 2011).

Table 6.6 Classification of Acceptable Risk

Immediate statistical:	
1. Natural	
a. Catastrophic	Involuntary
b. Ordinary	Involuntary
2. Man-originated	
a. Catastrophic	Voluntary and involuntary
b. Ordinary	Voluntary, regulated voluntary, and involuntary
3. Man-triggered	
a. Catastrophic	Involuntary
b. Ordinary	Voluntary, regulated voluntary, and involuntary
Immediate identifiable[a]	
Delayed statistical[a]	
Delayed identifiable[a]	

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011; Doro-on, A., Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX, 2009; Shih, C. and Riojas, A., Risk and its acceptability for groundwater contamination by hazardous wastes, in *Risk Assessment for Groundwater Pollution Control*, W. McTernan and E. Kaplan, eds., American Society of Civil Engineers (ASCE), Reston, VA, 1990, pp. 126–157; Rowe, W., *An Anatomy of Risk*, John Wiley & Sons, Toronto, Ontario, Canada, 1977.

[a] Same as immediate statistical.

6.3.8 Prerequisites for Risk Acceptance of Terrorist Attacks and Disaster

Before undertaking the development of a methodology for risk acceptance, a number of questions must be asked. "Is there a need for risk acceptance?" "How and where shall it be used?" "What methods and techniques are currently available?" "What alternative approaches can be employed?"

6.3.8.1 Requirement for a Methodology

Humans are naturally risk-aversive, but they are willing to take risks to achieve specific benefits and personal desires when the choice is under their direct control.

Table 6.7 Summary of Risk Reference

Risk Classification			*Class of Consequences*	
	Fatality/ Year	*Health Effects/ Year*	*Property Damage ($)/Year*	*Life Span Shortened/ Year*
Naturally occurring (act of God)				
Catastrophic	9.5×10^{-7}	4.8×10^{-6}	0.02	2.8×10^{-2}
Ordinary	6.8×10^{-5}	3.8×10^{-4}	2.8	0.2
Man-originated catastrophy				
Voluntary	1.8×10^{-6}	1.8×10^{-6}	0.38	5.8×10^{-3}
Regulated voluntary	2.8×10^{-5}	2.8×10^{-6}	0.38	5.8×10^{-2}
Involuntary	9.8×10^{-8}	4.8×10^{-7}	1.8	2.8×10^{-2}
Ordinary	4.8×10^{-6}	2.8×10^{-5}	1	9.5×10^{-3}
Involuntary	5.8×10^{-4}	2.8×10^{-1}	200	1
Voluntary	9.5×10^{-5}	5.8×10^{-2}	40	0.1
Regulated voluntary				
Man-triggered catastrophy				
Involuntary	1.8×10^{-7}	1×10^{-6}	3.8×10^{-2}	5.8×10^{-4}
Voluntary	3.8×10^{-6}	4×10^{-6}	0.75	5.8×10^{-3}
Ordinary	9.8×10^{-6}			2.8×10^{-2}
Involuntary	9.8×10^{-4}			1.8
Voluntary	1.8×10^{-4}			0.18
Regulated voluntary				

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011; Doro-on, A., Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX, 2009; Shih, C. and Riojas, A., Risk and its acceptability for groundwater contamination by hazardous wastes, in *Risk Assessment for Groundwater Pollution Control*, W. McTernan and E. Kaplan, eds., American Society of Civil Engineers (ASCE), Reston, VA, 1990, pp. 126–157; Shih, C.S. et al., *Risk Assessment of Terrorism Based on Prospect Theory for Groundwater Protection. Vol. 1 Environmental Science and Technology*, American Science Press, Houston, TX, 2007; Rowe, W., *An Anatomy of Risk*, John Wiley & Sons, Toronto, Ontario, Canada, 1977.

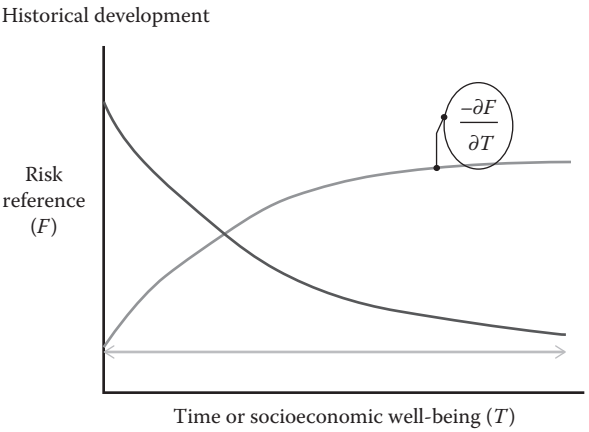


Figure 6.2 Risk reference versus socioeconomic well-being. (From Doro-on, A., Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX, 2009.)

When the risk is imposed by humans or nature as "acts of God" without immediate gain, however, risk-aversive action dictates. The subjects of the news reports, a reflection of society's news preferences, make it evident that society is more concerned with controversial and undesirable consequences than with benefits. Disaster or terrorism reports and political controversy news overshadow the news about achievements and health benefits.

The risk aversion of society, coupled with increasing awareness of new risks resulting from the side effects of new technology, has focused increased attention on technological risk. The side effects of new technology are probably irreversible, because the knowledge base for technology assessment and risk identification is available to everyone. Consideration of societal risk in all technological approaches in evaluating risk is estimated in two different theoretical models for regulatory approaches: (1) the rational model and (2) the bureaucratic model.

6.4 Establishing the Risk Referent

Sections 6.4.1 through 6.4.5 illustrate the systematic procedures for developing the risk referent.

6.4.1 Multiple Risk Referents

Different types of risk can be analyzed through the absolute risk levels for involuntary risk and for regulated voluntary risk. Moreover, risks can be compared and

balanced across equivalent indirect gains at a certain degree to create final risk values, for the activity is correlated with every equivalent type of risk as referent. When all quantified risks are lesser than their risk referent counterparts, the net calculated risks are acceptable. If any risk exceeds the referents, then the net calculated risks are unacceptable, and therefore risk reduction shall be employed to make them acceptable.

For the weighting factor of cumulative prospect theory, $\omega(p)$, the considerations of the degree of voluntarism ($F1$), benefit–cost balance to the society ($F2$), and controllability of risk ($F3$) will be included and quantified (Doro-on 2009, 2011). Furthermore, the risk as defined by cumulative prospect theory is essentially the risk referent, which is the incremental acceptable risk of the US society: risk referent = $F1 \times F2 \times F3 \times$ risk reference (Doro-on 2009, 2011).

6.4.2 Risk Proportionality Factor Derivation from Risk References

In utilizing risk references, it is expected that there is a proportion of total societal risk that is acceptable to society (societal value judgment) to gain indirect benefit, and is called a *risk proportionality factor*. For example, a greatly beneficial plan to society such as the termination of heart disease and breast cancer as the cause of death might totally lessen the life span of those not affected by heart disease and breast cancer, as the resultant lower death rate might increase the age of the population and the competition for limited resources.

As a value judgment, an extremely beneficial plan to the society could be acceptable if the increase of net involuntary societal risks were less than 9% of the overall degree of involuntary risk. This value can be used as a top level for the risk proportionality factor for involuntary risk. In this case, the risk of terrorist attacks against pipelines, tunnels, underground rail, and transit systems including clandestine manpower mobilization and illegal secret fabrications of WMD will be compared to "accidents" to analyze risk and quantify risk acceptability.

If there are no other alternatives available, one expects to assume a greater proportion of risk, or it can be equivalent to all other risks. The author of this book has made an engineering judgment of 0.09 for the risk proportionality factor for involuntary risk and a value of 1.0 for the voluntary or regulated voluntary risk.

There are two differences in voluntary risk: One group of risks involves the operator or controller of a technological system (e.g., a high-speed underground maglev train; UMT). The second group involves the population that is at voluntary risk, with appropriate alternatives available (e.g., UMT passengers). In this case, the first group of voluntary risks is the operator or driver, and the second, the society, or passengers. Although voluntary absolute risk levels are used for examining the second type of voluntary risk, a risk proportional factor of 0.09 is proposed. If the society is risk-aversive, it will reject large risks if alternatives are achievable.

Table 6.8 Risk Proportionality (*F*1) and Derating Factors (*F*2)

	Involuntary	*Regulated*
Factor	*Risk*	*Voluntary*
Proportionality factor (*F*1)	0.09	1.0
Derating factor (*F*2)		
Balance		
Favorable	1.0	1.0
Marginal favorable	0.09	0.18
Indecisive	0.0081	0.09
Marginal unfavorable	0.00073	0.018
Unfavorable	0.000065	0.009

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011; Doro-on, A., Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX, 2009; Rowe, W., *An Anatomy of Risk,* John Wiley & Sons, Toronto, Ontario, Canada, 1977.

6.4.3 Risk Proportionality Derating Factors

A second group of social value judgments is to identify the risk proportionality derating factors for smaller favorable indirect gain–loss balances. The five conditions of indirect gain–loss balance are presented in Table 6.8: (1) favorable balance, (2) marginal favorable balance, (3) indecisive balance, (4) marginal unfavorable balance, and (5) unacceptable balance. Take note: A factor of 1.0 represents a doubling of existing risk for the new proposed scheme. A factor of 0.09 is 9% of the current risk. In this book, the derating functions shown in Table 6.9 have been selected as "straw men" values.

6.4.4 Degree of Systemic Control

The degree of risk that society is tolerating in the current situation is not always acceptable to society, or the society may not be satisfied with the current level of risks. In this condition, the society will want to minimize the risk compared to the current level of risk. The author has used the values derived in Table 6.9 for the risk controllability factor *F*3, which is the product of the four factors listed in Table 6.9.

Table 6.9 Controllability Factors (*F3*)

Control Approach		*Degree of Control*		*State of Implementation*		*Control Effectiveness*	
Factor	*C1*	*Factor*	*C2*	*Factor*	*C3*	*Factor*	*C4*
Systemic control	1.0	Positive	1.0	Demonstrated	1.0	Absolute	1.0
Risk management system	0.80		0.80		0.80		0.80
Special design features	0.55		0.55	Proposed	0.55	Relative	0.55
Inspection and regulation	0.25	Level	0.25		0.30		0.30
		Negative	0.18		0.2		0.2
No control scheme	0.08	Uncontrolled	0.08	No action	0.08	None	0.08

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Boca Raton, FL, 2011; Doro-on, A., Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system, PhD dissertation, University of Texas at San Antonio, San Antonio, TX, 2009; Rowe, W., *An Anatomy of Risk*, John Wiley & Sons, Toronto, Ontario, Canada, 1977.

6.4.5 Conversion of a Risk Reference to a Risk Referent

The conversion of a risk reference to a risk referent requires three factors:

1. Establish the appropriate *risk proportionality factor*, that is, the fraction of existing societal risk, also known as *risk reference*, which would be considered acceptable in a condition where there was a very favorable indirect benefit–cost balance, for both regulated voluntary (or voluntary) and involuntary risks ($F1$).
2. Establish a factor which is the *risk proportionality derating factor*, which can be applied in those conditions where the indirect benefit–cost balance is not as favorable, and which transforms the *risk proportionality factor* in those identified conditions ($F2$).
3. Establish the modification factor related to the degree of risk controllability ($F3$).

Using the three aforementioned factors, calculate the risk referent, which is the incremental acceptable risk $V(f)$ (in cumulative prospect theory) based on the current socioeconomic well-being in the United States (or in any other society, country, or nation).

$$\text{Risk referent} = \text{Risk reference} \times F1 \times F2 \times F3 \tag{6.4}$$

The first two factors deal with the fundamental propensity of individuals and/or groups to take risks and integrate the additional decision aspect of indirect benefits/costs. This acknowledges the tendency for people to accept a higher level of risk if the benefit to them more than offsets the imposed risk or for people to be increasingly risk-aversive in the opposite case. All three of these factors are based on value judgments. The specific numbers in Table 6.8, risk proportionality and proportionality derating factor ($F1$ and $F2$), and Table 6.9, controllability factor ($F3$), are based on the straw men values originally posed by Rowe (1977) and modified in this book based on the author's scientific and engineering judgment.

The overall controllability factor is the result of a multiplication of four subfactors ($F3 = C1 \times C2 \times C3 \times C4$).

The four subfactors are as follows:

1. Control approach (i.e., the type of risk control management used)
2. Degree of control (i.e., effectiveness of risk control)
3. State of implementation
4. Basis for control effectiveness

Moreover, the relationships of cumulative prospect theory and risk referents are as follows (Doro-on 2009, 2011):

$$V(f) = \omega(p) \cdot v(x) \quad \left(\text{from Equation } 6.3\right)$$

$$\text{Risk referent} = \{\boldsymbol{F}1 \times \boldsymbol{F}2 \times \boldsymbol{F}3\} \times \text{risk reference}$$

where

$V(f)$ is the risk referent
$\omega(p) = \{F1 \times F2 \times F3\}$
$v(x)$ is the risk reference

Therefore,

incremental risk acceptability = $V(f)$ = Risk referent

$$V(f) = \{F1 \times F2 \times F3\} \times \text{risk reference} \tag{6.5}$$

Examples of screening alternatives using the incremental risk acceptability are presented in Chapter 7.

6.5 Implication

The practice of risk acceptability based on quantitative psychology is really vital in homeland security and defense in order to select the stronger deterrent and defensive systems against potential attacks (man-made disaster) and natural disasters. Improvement to intelligence and emphasis on military support to homeland protection are both essential in maintaining safety and security. Chapter 7 demonstrates a concise strategic intelligence analysis, presents military support, and discusses military intuitive judgment. Examples of the risk assessment methodologies discussed in Chapters 5 and 6 including graphical illustrations of terrorism activity scenarios and preventive/defensive measures are also demonstrated in Chapter 7.

References

Callan, S. J. and Thomas, J. M. 2010. *Environmental Economics & Management: Theory, Policy, and Applications*, 5th edn. Mason, OH: South-Western Cengage Learning.

Dimitri, N. and van Eijck, J. 2012. *Games, Actions, and Social Software: Time Discounting and Time Consistency*. Berlin, Germany: Springer-Verlag, p. 29.38. http://homepages.cwi.nl/~jve/papers/11/pdfs/tdChapter.pdf (accessed January 3, 2013).

Doro-on, A. 2009. Risk assessment embedded with cumulative prospect theory for terrorist attacks on aquifer of karstic limestone and water supply system. PhD dissertation, University of Texas at San Antonio, San Antonio, TX.

Doro-on, A. 2011. *Risk Assessment for Water Infrastructure Safety and Security*. Boca Raton, FL: CRC Press.

Easterlin, R. 1974. "Does Economic Growth Improve the Human Lot?" in Paul A. David and Melvin W. Reder, eds., Nations and Households in Economic Growth: Essays in Honor of Moses Abramovitz, New York: Academic Press, Inc.

Fraisse, P. 1984. Perception and estimation of time. *Annu. Rev. Psychol.* 35:1–36.

Frank, R. 1997. "The Frame of Reference as a Public Good", *The Economic Journal 107* (November), 1832–1847.

Fredrickson, B. L. and Kahneman, D. 1993. Duration neglect in retrospective evaluations of affective episodes, *J. Pers. Soc. Psychol.*, 65 (July), 44–55.

Higgins, E. T. 1996. Knowledge activation: Accessibility, applicability, and salience. In *Social Psychology: Handbook of Basic Principles*, eds. E. Tory Higgins and Arie W. Kruglanski, pp. 133–168. New York: Guilford Press.

Kahneman, D. 2003. Maps of bounded rationality: Psychology for behavioral economics. *Am. Econ. Rev*. 93(5):1449–1475. http://www.princeton.edu/~kahneman/docs/Publications/Maps_bounded_rationality_DK_2003.pdf (accessed October 3, 2012).

Kahneman, D. 2011a. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

Kahneman, D. 2011b. Slow down you think too fast. http://bigthink.com/ideas/41419 (accessed January 22, 2013).

Kahneman, D. 2012. Slow Down You Think Too Fast. http://bigthink.com/videos/slow-down-you-think-too-fast-2 (accessed November 1, 2012).

Kahneman, D. and Frederick, S. 2002. Representativeness revisited: Attribute substitution in intuitive judgment. In *Heuristics and Biases: The Psychology of Intuitive Though*t, eds. T. Gilovich, D. Grifin, and D. Kahneman, pp. 49–81. New York: Cambridge University Press.

Kahneman, D. and Klein, G. 2009. *Conditions for Intuitive Expertise*. Princeton, NJ: Princeton University. http://www.fiddlemath.net/stuff/conditions-for-intuitive-expertise.pdf (accessed November 1, 2012).

Kahneman, D., Knetsch, K., and Thaler, R. 1990. Experimental tests of the endowment effect and the Coase theorem. *J. Polit. Econ*. 98(6):1325–1348.

Kahneman, D., Knetsch, J., and Thaler, R. 1991. The endowment effect, loss aversion, and status quo bias: Anomalies. *J. Econ. Perspect*. 5(1):193–206.

Kahneman, D., Ritov, I., and Schkade, D. 1999. Economic preferences or attitude expressions? An analysis of dollar responses to public issues. *J. Risk Uncertain*. 19(1–3):203–235.

Kahneman, D., Slovic, P., and Tversky, A. (eds.). 1982. *Judgment Under Uncertainty: Heuristics and Biases*. New York: Cambridge University Press.

Kahneman, D. and Tversky, A. 1973. On the psychology of prediction. *Psychol. Rev*. 80(4):237–251.

Kahneman, D. and Tversky, A. 1979. Prospect theory: An analysis of decision under risk. *Econometrica* 47(2):263–292.

Kahneman, D. and Tversky, A. 2000. *Choices, Values and Frames*. New York: Russell Sage Foundation.

Nogami, G. and Streufort, S. 1973. Time effects on perceive risk taking. Purdue University Technical Report No. 11, Lafayette, IN.

Otway, H. 1975. Risk assessment and societal choices, IIASA RM-75-2. International Institute for Applied Systems Analysis, p. 7. Laxenburg, Austria.

Read, D. and Loewenstein, G. 1995. The Diversification Bias: Explaining the Difference between Prospective and Real-time Taste for Variety, *Journal of Experimental Psychology:* 40 *Applied*, 1 (1), 34–49.

Rowe, W. 1977. *An Anatomy of Risk*. Toronto, Ontario, Canada: John Wiley & Sons.

Rubenstein, A. 1979. False probabilistic arguments vs. faulty intuition. *Isr. Law Rev*. 14:247–254.

Saks, M. J. and Kidd, R. F. 1981. Human information processing and adjudication: Trial by heuristics. *Law Soc. Rev*. 15:123–160.

Sherover, C. 1975. *The Human Experience of Time: The Development of Its Philosophic Meaning*. New York: New York University Press.

Shih, C. and Riojas, A. 1990. Risk and its acceptability for groundwater contamination by hazardous wastes. In *Risk Assessment for Groundwater Pollution Control*, eds. W. McTernan and E. Kaplan, pp. 126–157. Reston, VA: American Society of Civil Engineers (ASCE).

Shih, C. S., Doro-on, A., and Arroyo, G. A. 2007. *Risk Assessment of Terrorism Based on Prospect Theory for Groundwater Protection. Vol. 1 Environmental Science and Technology*. Houston, TX: American Science Press.

Stanovich, K. and West, R. 2000. Individual differences in reasoning: Implications for the rationality debate? *Behav. Brain Sci*. 23(5):645–665.

Thagard, P. 2012. Should you trust your intuitions? http://www.psychologytoday.com/blog/hot-thought/201203/should-you-trust-your-intuitions (accessed November 11, 2012).

Turetzky, P. 1998. *Time*. London, UK: Routledge.

Tversky, A. and Kahneman, D. 1974. Judgment under uncertainty: Heuristics and biases. *Science* 185(4157):1124–1131.

Tversky, A. and Kahneman, D. 1981. The framing of decisions and the psychology of choice. *Science* 211(4481):453–458.

Tversky, A. and Kahneman, D. 1983. Extension versus intuitive reasoning: The conjunction fallacy in probability judgment. *J. Bus*. 90(4):293–315. http://www.econ.ucdavis.edu/faculty/nehring/teaching/econ106/readings/extensional%20versus%20intuitive.pdf (accessed October 2, 2012).

Tversky, A. and Kahneman, D. 1986. Rational choice and the framing of decisions. *J. Bus*. 59(4):S251–S278.

Tversky, A. and Kahneman, D. 1991. Loss aversion in riskless choice: a referencedependent model. *Quarterly Journal of Economics*, 106(4), 1039–1061.

Tversky, A. and Kahneman, D. 1992. Advances in prospect theory: Cumulative representation of uncertainty. *J. Risk Uncertain*. 5:297–323; http://3xfund.com/images/article009.pdf (accessed January 5, 2006).

US Environmental Protection Agency. 1973. *The Quality of Life Concept: A Potential New Tool for Decision Makers*. Washington, DC: Office of Research and Development. http://nepis.epa.gov/Exe/ZyNET.exe/20016RYI.PDF?ZyActionP=PDF&Client=EPA&Index=Prior%20to%201976&File=D%3AZYFILESINDEX%20DATA70THRU75TXT0000000520016RYI.txt&Query=000R73002%20or%20The%20or%20Quality%20or%20Life%20or%20Concept%20or%20A%20or%20potential%20or%20New%20or%20Tool%20or%20for%20or%20Decision%20or%20Makers%20or%20USEPA&SearchMethod=1&FuzzyDegree=0&User=ANONYMOUS&Password=anonymous&QField=pubnumber∩%22000R73002%22&UseQField=pubnumber&IntQFieldOp=1&ExtQFieldOp=1&Docs (accessed May 10, 2009).

US Environmental Protection Agency. 2009. Quality of life indicators. http://www.epa.gov/reva/seql_qol.html (accessed May 10, 2009).

Velimirovic, H. 1975. An anthropological view of risk, IIASA RM-75-55. International Institute for Applied Systems Analysis, Laxenburg, Austria. p. 17.

Wilson, R. 1975. Examples of risk-benefit analysis. *CHEMTECH—J. Am. Chem. Soc*. P604–P607.

Chapter 7

Strategic Intelligence Analysis, Military Support, and Military Intuitive Judgment in Safeguarding Pipelines, Tunnels, Underground Rail and Transit Operations, and Homeland

7.1 Introduction

This chapter unequivocally demonstrates the integration of *risk assessment and acceptability analysis based on the quantitative psychology of intuitive judgments to intelligence analysis and sound military decision* in support of the protection of pipelines, tunnels, underground rail, and transit operations including the analysis of clandestine tunnels and operations for weapons of mass destruction (WMD) production and terror-military mobilization of enemies and rebellious

nations. Illustrative examples for this approach are presented in this chapter. After a decade of guerrilla warfare in Afghanistan and Iraq, the military is refocusing on the wider world, particularly the Pacific (Freedberg 2013). On February 12, 2013, North Korea has carried out its third, most powerful nuclear test despite United Nation warnings (BBC News 2013). In the past, the United States confronted North Korea about its alleged clandestine uranium enrichment program (Squassoni 2006). US intelligence officials claimed that Pakistan was a key supplier of uranium enrichment technology to North Korea, and some media reports suggested that Pakistan had secretly exchanged centrifuge enrichment technology for North Korean help in developing longer-range missiles (Squassoni 2006). Moreover, North Korea is widely believed to have mastered the engineering requirements of plutonium production a decade ago and by approximation it is estimated that North Korea has between 30 and 50 kg of separated plutonium, enough for at least half a dozen nuclear weapons (Nikitin 2013). Historically, a wide range of US military and dual-use goods are illegally transshipped to Iran through United Arab Emirates, Malaysia, Singapore, and other countries, according to US officials (GAO 2010). Nuclear smuggling in its global ramifications represents a recurrent and dangerous threat to international security and stability (Lee 2008). The intelligence estimation process needs to take into account the vast potential of the black market for supplying adversaries with nuclear-related and other WMD items (Lee 2008). Meanwhile, the enemies and rebellious nations have goals and are planning for future intimidation, conflicts, and a high magnitude of terror attacks, while they also develop their own strategic intelligence and military support operations to be able to successfully launch WMD and defend themselves. There is a demand for threat assessment and warnings, identification of terrorism scenarios that can be used for rapid collection of information, intelligence, and military intuitive recognitions.

7.2 Intelligence Analysis

Intelligence is a primary vehicle of effectively predicting the enemies and rebellious nations' dangerous secret terrorism activities, and it cleverly aids in identifying their specific targets aiming at their ultimate goal of gaining power and winning against the United States, allies, and friendly nations. Nonetheless, it also traces routes of terror operations and leads to accurate calculation of the enemy's actions when delivered intelligently. The outstanding progress in intelligence collection mechanisms has expanded the opportunity of *combat zone* information from ample sources. Salient combat zone information becomes beneficial to the preparation of war games against the enemy when it is quantitatively exploited and synthesized. The information resulting from analyzing combat zone information becomes intelligence. According to the Central Intelligence Agency (CIA 2007), intelligence analysis is the application of individual and

collective cognitive methods to weigh data and test hypotheses within a secret sociocultural context. Extensively, the intelligence analyst correlates pieces of information from diverse sources for fabrication of a precise picture of the combat zone. A combat zone plan of terrorism in oil and gas pipelines is presented in Figure 7.1. Thus, analysis produces the intelligence that is critical to reach attainable success in combating against the enemy.

There are four divisions of intelligence services that aid homeland security and defense: foreign intelligence, domestic intelligence, defense intelligence, and criminal intelligence. According to US Joint and National Intelligence (JNI 2012), the Department of Defense (DoD) has instituted several changes to the DoD intelligence community (IC) since the terrorist attacks on the United States in September 2001. In war, intelligence focuses on enemy military capabilities, centers of gravity (COGs), and potential courses of action (COAs) to provide operational and tactical commanders the information they need to plan and conduct operations (JNI 2012). At the strategic level, intelligence facilitates nonproliferation activities and the development of effective counterproliferation plans by providing intelligence of activities between suppliers of WMD (and their associated materials, technology, and expertise necessary to create and sustain a WMD program) and state and nonstate actors attempting to acquire WMD by providing assessments of adversary WMD capabilities (JNI 2012). Intelligence provides warning of WMD attacks and is vital to WMD threats and locating WMD and/or toxic industrial materials (TIMs) (chemical, biological, or radiological; refer to Chapter 2) in the area of concern is a critical aspect as the presence of these elements can create an environment requiring extraordinary protection and produce long-term health hazard with massive environmental damage (JNI 2012).

In combating urgent threats of WMD, defense intelligence is critical to the DoD's role in national security and such information helps frame national security policies, and enables warfighters to plan and conduct successful military and security operations to protect America (DoD 2013), including its allies and friendly nations. The success of intelligence, surveillance, and reconnaissance (ISR) systems in collecting, processing, and disseminating intelligence information has fueled a demand for ISR support, and the DoD has significantly increased its investments in ISR capabilities since combat operations began in 2001 (GAO 2011).

While the Defense Intelligence Agency's (DIA) core mission resides in four intelligence competencies: all-source analysis, counterintelligence (CI), human intelligence (HUMINT), and measurement and signatures intelligence (MASINT) (DIA 2011). Primarily focused on foreign military and defense-related matters, DIA will (DIA 2011)

- Provide strategic warning and integrated risk assessment
- Plan and direct defense intelligence activities for all-source analysis; collection management; ISR; HUMIN; CI; OSINT; MASINT; technical collection; and international engagement

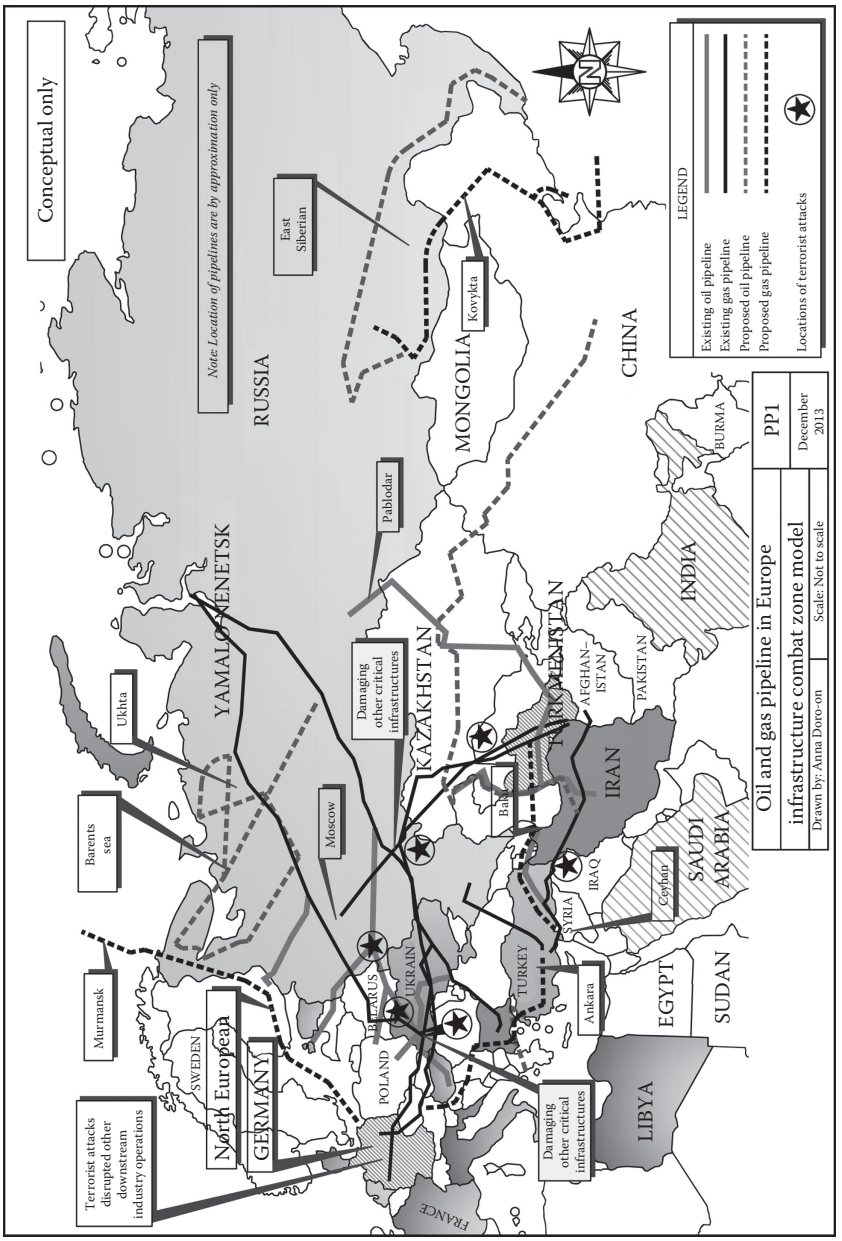


Figure 7.1 Example of an infrastructure combat zone—oil and gas pipelines.

- Collect information through HUMINT, CI, OSINT, MASINT, and technical means
- Process and exploit information
- Produce all-source intelligence analysis from all available means of collection
- Integrate and disseminate defense intelligence products and data

7.3 Standard Intelligence Analysis Cycle

Intelligence operations follow a five-phase process known as the *intelligence cycle*. It is a concept that describes the fundamental cycle of intelligence processing in a civilian or military intelligence agency or in law enforcement as a closed path consisting of repeating nodes (CIA 2010a). It consists of six interrelated categories of intelligence operation (DOA 2012): (1) planning and direction; (2) collection; (3) processing and exploitation; (4) analysis and production; (5) dissemination and integration; (6) evaluation and feedback. The phases of the intelligence cycle include the issuance of requirements by decision makers, commanders, and the collection, processing, analysis, and publication of intelligence. The circuit is completed when decision makers or commanders provide feedback and revised requirements. The conventional intelligence cycle is presented in Figure 7.2. The intelligence process supports all the activities of the operation process (plan, prepare, execute, and assess) and can be conducted multiple times to support each activity of the operation process (DOA 2012).

According to Rob Johnston (2005), the traditional intelligence cycle model should be redesigned to depict accurately the intended mission. Erroneous information and doctrine simply lead to poor judgments that can result in incompetent performance, confusion, disorganization, and a need for reteaching. If the primary goal is to capture the overall intelligence process from the request for a product to its production and conveyance, including the enterprises of IC members, then essentially a greater deal is required. This should be a model that pays particular attention to representing accurately all the elements of the process and the factors that influence them (Johnston 2005; CIA 2010b). The model omits elements and fails to capture the process accurately and a standard intelligence cycle model should be either redesigned to depict accurately the intended goal or care should be taken to discuss explicitly its limitations whenever it is used (Johnston 2005). In this chapter, the modified intelligence analysis is presented in Figure 7.3, which entrenches the risk assessment methodology presented in Chapters 5 and 6. Intelligence reduces operational uncertainty by providing information and predictive assessments on those elements of the military problem that the commanders can least control (DOA 2012).

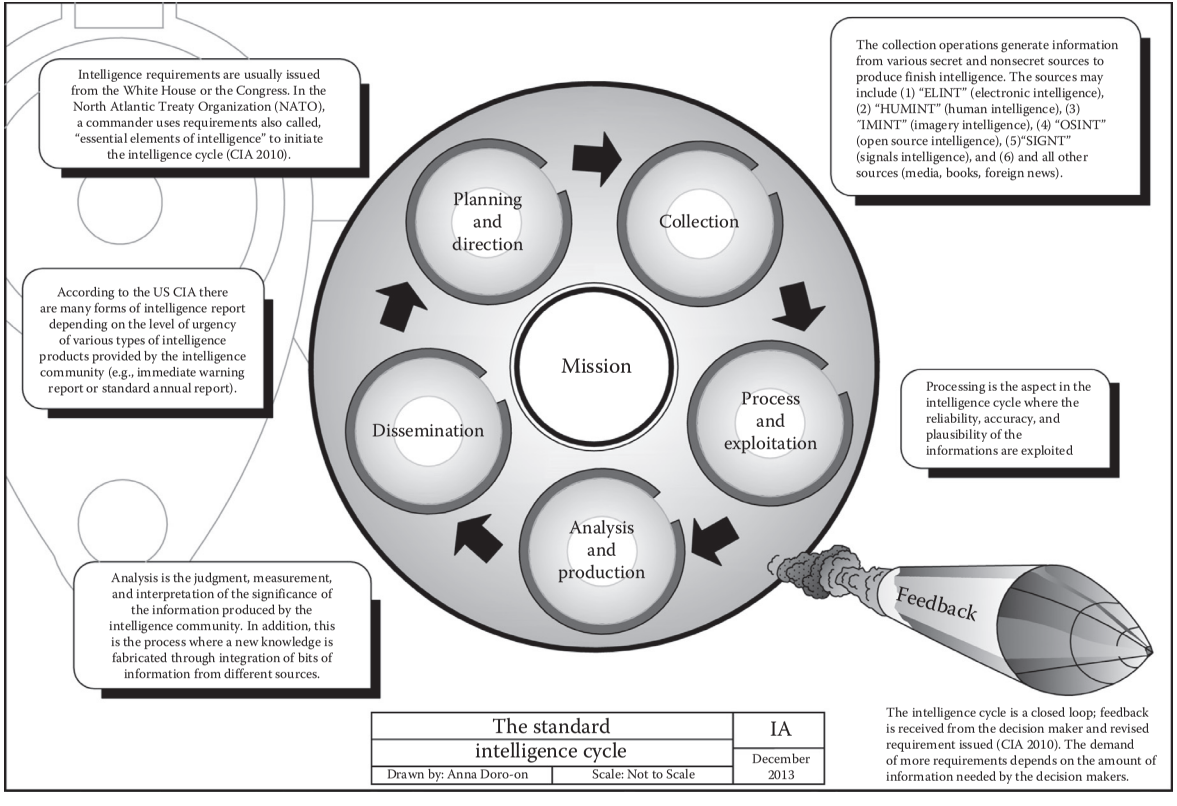


Figure 7.2 Standard intelligence cycle. (From Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2011.)

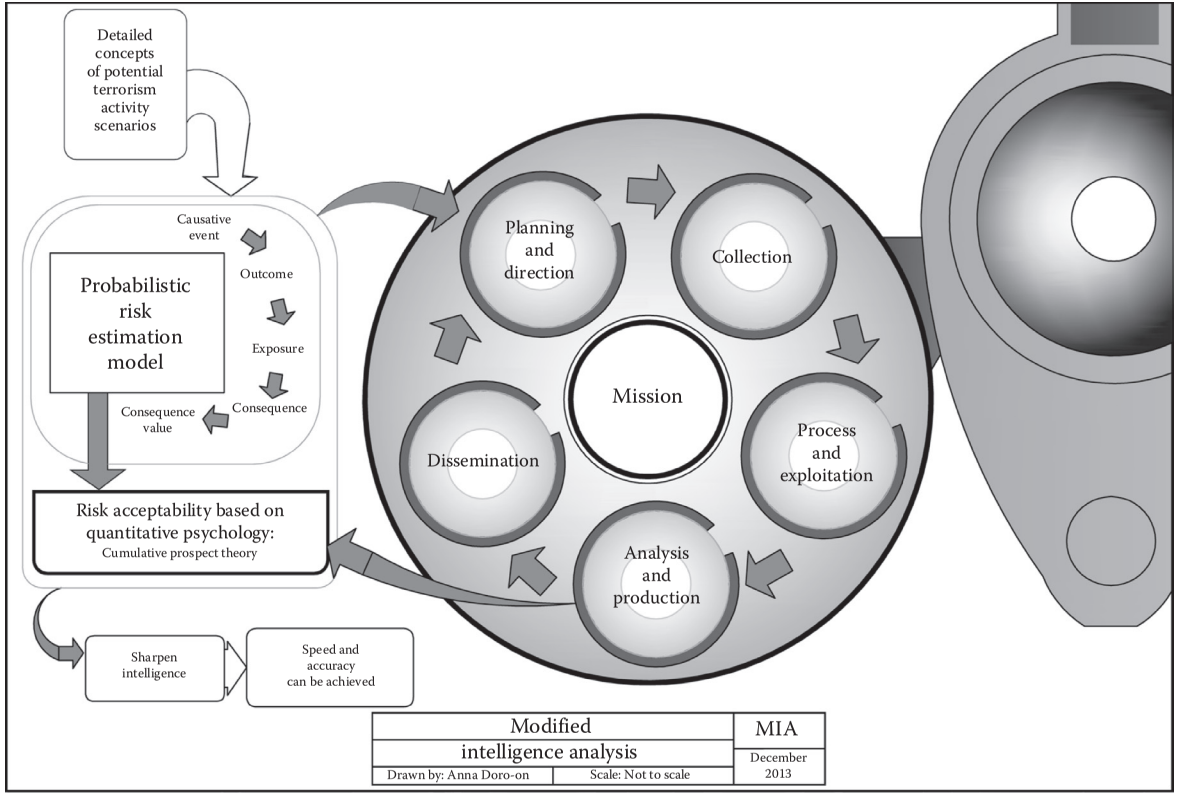


Figure 7.3 Modified intelligence analysis process. (From Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2011.)

7.4 Quantitative Risk Estimation for the Intelligence Analysis of Infrastructure Protection and WMD Mitigation

The risk estimation model presented in Chapter 6 is utilized to develop succinct combat zone configurations for intelligence analysis to

- Provide terrorism threat assessments and warnings
- Provide guidance for unique combat requirement
- Provide concise critical information requirements
- Synchronize the intelligence combat employment
- Discern the enemy's activities and terror-military operations with accuracy
- Understand the topographical, geological (e.g., underground tunnels), and meteorological conditions (i.e., weather) that surrounded the situations
- Consider employing Mother Nature (discussed in Section 8.13)
- Consider employing Mother Nature with intelligent devices before and during the launch of weapons (detailed in Section 8.13)
- Predict the enemy's preventive and defense systems
- Recognize the enemy's subterranean and clandestine locations for evasion
- Create awareness of civilian/public safety
- Provide proper employment with synchronization of assets to defeat the enemy
- Develop new assets rapidly and to plan to meet combat requirements against urgent threats
- Provide effective collaboration with allies and friends
- Minimize risk and optimize acceptable risk of the security, defensive, and offensive operations

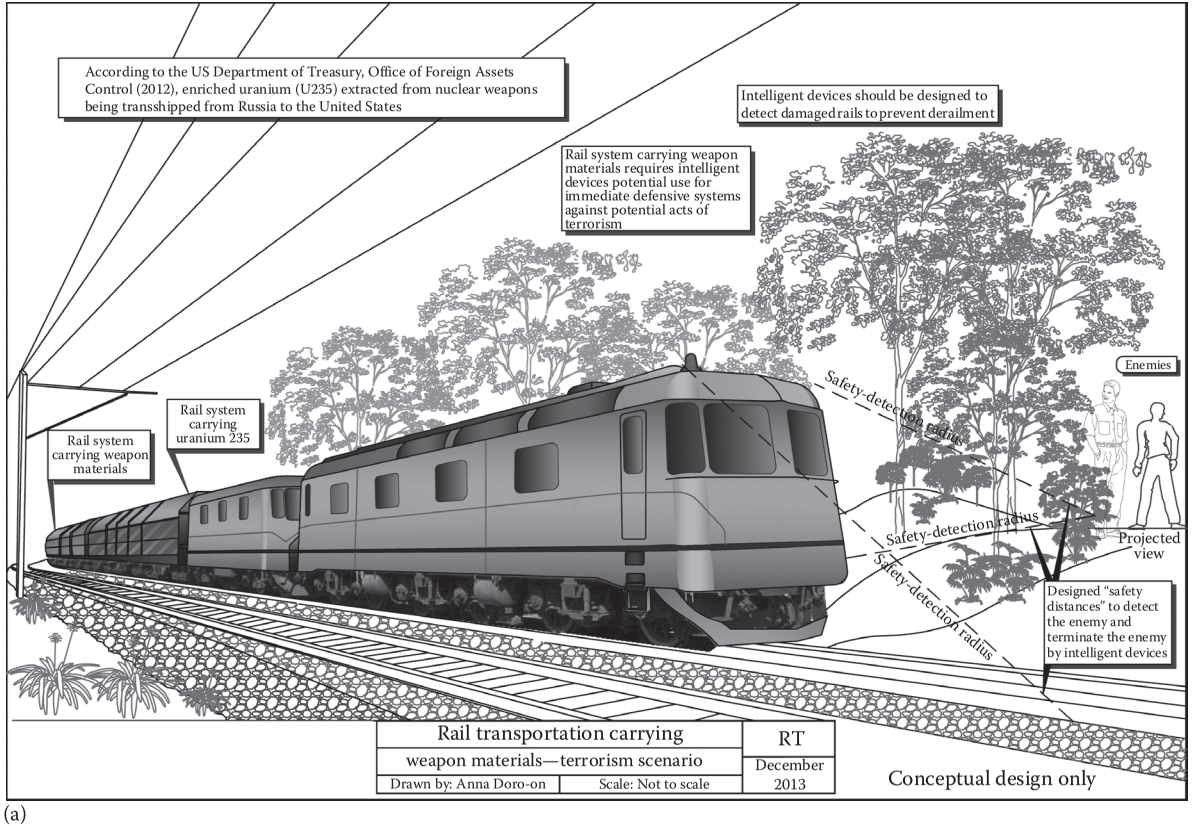
Additionally, the *risk estimation model* will be developed based on the event tree analysis and probabilistic model (refer to Chapter 5). The five steps of risk estimation process to aid intelligence analysis for terror attacks on the rail system for transshipment of nuclear bomb materials and illegal secret production and transshipment of WMD (i.e., chemical, biological, radiological, and nuclear; refer to Chapter 2) materials with illustrative examples are also presented here.

7.5 Intelligence Analysis Development: Risk Estimation Models for Rail System Threat and Intuitive Predictions for the Smuggle of WMD Components and Clandestine Terror-Military Operations

Terrorist groups have been waiting for the opportunity to attack rail systems carrying nuclear bomb materials to steal and generate disaster similar to or greater than

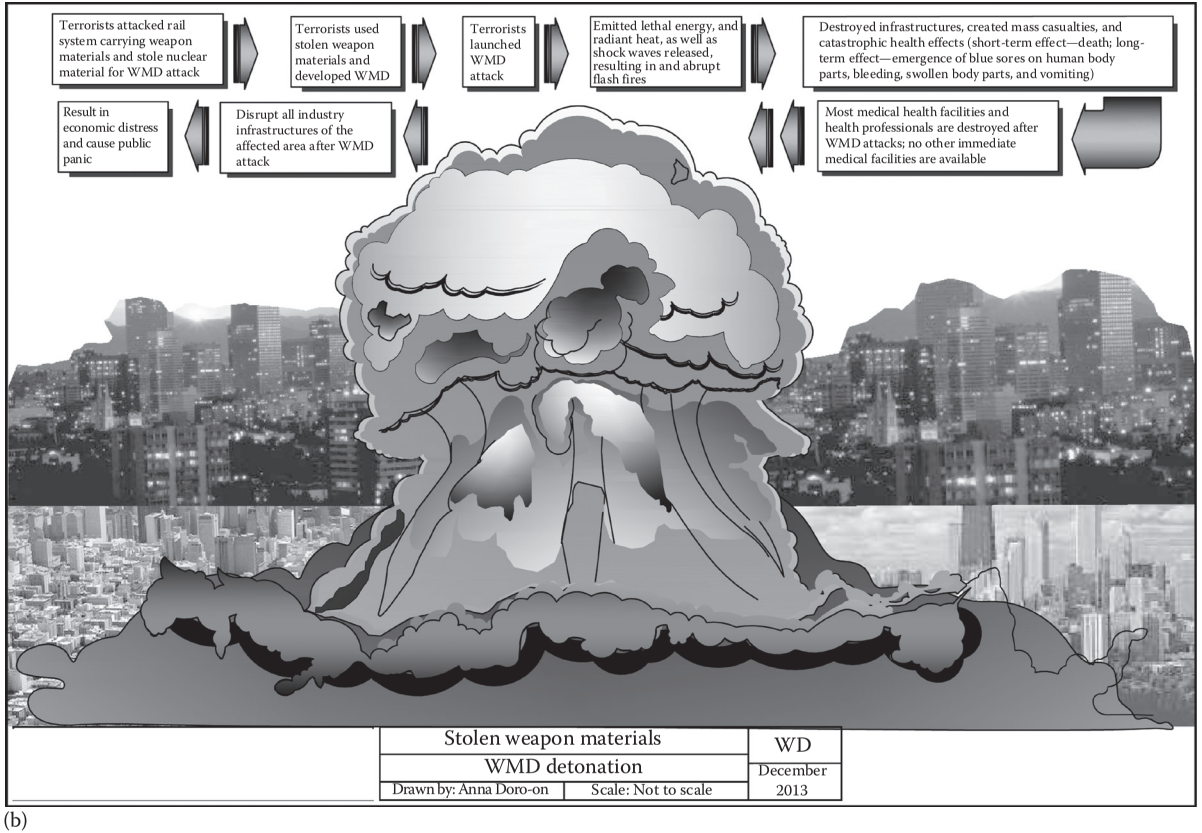
the degree of damage created by terrorism on September 11, 2001. The following reasons conceptualize the possibility of a successful terrorism against rail systems:

- Inadequacy of devices (e.g., intelligent detection and defense devices to counter explosive devices) and intuitive techniques for infrastructure protection and defense against improvised weapons.
- No thorough investigation or detection conducted on individuals purchasing large amounts of gasoline in local gasoline stations.
- Lack of intelligent devices to deter and defend the rail system carrying hazardous material (HAZMAT), weapon materials, and other materials for the military used against sabotage.
- Deficiency in regulations enforcing effective *protective systems* against terrorism or other man-made disaster for tunnels, rails, and transit systems.
- It only requires approximately 75 lb of enriched uranium (U235) to make a fission weapon, or 55 lb of natural uranium (99.3% U238 + 0.7% U235) to build one weapon, or 10–22 lbs of plutonium (Pu239) to make one fission weapon for a mass atrocity or mass genocide. For instance, if a rail system is carrying 1 ton of U235, 1 ton can produce at least 26 WMD. There should be a better way to secure rail systems carrying *classified* (bomb) materials. Security is not enough—a defense system should be prepared with *safety distance* (*encroachment*) considerations in the event of terrorist attacks. According to the US Department of Treasury, Office of Foreign Assets Control (2012), U235 was extracted from nuclear weapons being transshipped from Russia to the United States for commercial nuclear reactors (example of bomb materials transshipment is presented in Figure 7.4a).
- Insufficient security surveillance in the vicinity adjacent to or neighboring the rail, transit, and tunnel systems.
- A similar scenario was presented in Chapter 5 regarding illegal production of WMD, for which the conceptual reasons are listed later.
- Lack of hard evidence to convince the international regulators and agencies that the enemies were able to negotiate and acquire weapon materials from other corrupt nations or organizations.
- Lack of hard evidence to validate the enemies' *devious motives* for developing these potential WMD technologies. If strong proof existed that these nations and terrorists acquired WMD materials, proving their secret motives to be harmful to national and international security is not simple (Tables 7.1 through 7.6).
- Deficiency in international policy and security to prevent *illegal* commerce, transshipment, and production of WMD materials (Figure 7.4a) and WMD attack (Figure 7.4b).
- Lack of practice in *intuitive judgments and sound predictions* by some of the decision-makers, analysts, and international organization leaders in detecting and deterring the enemies from fabricating of WMD (Figure 7.5).



(a)

Figure 7.4 (a) Transshipments of classified materials.



(b)

Figure 7.4 (continued) (b) Terrorist attack using stolen WMD.

Table 7.1 Process of Risk Estimation for Rail System; Step 1: Causative Events

Step 1: Causative events	
a.	Terrorists' intrusion into the pathway of rail transportation system carrying bomb materials
b.	Terrorists' intrusion into tunnel of rail system
c.	The terrorist leaders and supporters provided description and identified the routine pathways and locations of rail transportation system carrying nuclear bomb materials

Table 7.2 Process of Risk Estimation; Step 2: Outcome

Step 2: Outcome	
a.	Terrorists took over the rail transportation system
b.	Generating rail transportation system accidents with explosive devices
c.	Rail transportation system rupture
d.	Ignition flammable material on rail system
e.	Generate rail derailment and collision
f.	Generate electromechanical failure and cyber control failure

7.6 Intelligence Analysis: Event Tree Analysis Model

Event tree analysis provides a logical assessment with graphical illustrations of sequential events resulting in significant outcomes, usually outcomes from a potential accident or disaster. It is also a binary form of a decision tree for evaluating the various multiple decision paths in a given problem (Ericson 2005). The event tree analysis for intelligence analysis is presented in Figure 7.6a through d. The *designed probability scales* for critical infrastructure analysis and intelligence analysis are provided in Tables 7.7 and 7.8, respectively. The risk rates based on the designed probability scales used in the event tree analysis for intelligence process are provided in Table 7.9. The issue in balancing risk assessment within the intelligence process is whether *risk is acceptable or not*, particularly dealing with urgent threats related to WMD. This is undeniably correct when national security issues are involved. Risk can be quantified based on a stochastic model describing all the events leading to grave consequences (i.e., WMD launch). However, public risk acceptability demands a profound understanding of the *anatomy of the perception of risks* as detailed in Chapter 7, Section 7.7, which demonstrates the cumulative prospect theory concept in quantitative psychology of intuitive judgments.

Table 7.3 Process of Risk Estimation for Rail System; Step 3: Exposure

Step 3: Exposure	
a.	HAZMAT including radioactive material dispersion in the environment after the explosion of transit systems: i. HAZMAT mixed in the atmosphere and the environment ii. HAZMAT will not be treated easily iii. HAZMAT mixed with other pollutants present in the environment iv. HAZMAT diluted in some areas via strong winds
b.	Explosions of transit systems created by explosive devices: i. Derailment and explosions of debris from transit systems and bomb components ii. Generation of debris and environmental contamination
c.	Terrorists successfully stole some nuclear bomb materials: i. Terrorists acquired nuclear weapon materials
d.	Rupture of rails and freights after strong collisions: i. Flash and pool fires during rail system disasters

Table 7.4 Process of Risk Estimation; Step 4: Consequence

Step 4: Consequence	
a.	Health effects (of the affected area) Short-term effect: Death Long-term effects: Impaired human health (impaired immune functions, cause various cancers, radiation poisoning and generate)
b.	Injury to the environment due to the release of HAZMAT, radioactive materials, and debris
c.	Cause damage to public morale and confidence due to the fear of WMD explosion by terrorists
d.	Mass casualties
e.	Pollute the environment and cause destruction of natural resources dependent on clean environment (after the release of HAZMAT)
f.	Collapse of key transportation system infrastructure
g.	Result in public and economic distress due to the need for urgent security against WMD explosion

Table 7.5 Process of Risk Estimation; Step 5: Consequence Values

Step 5: Consequence values	
a.	Protection and security policy revision
b.	Provide detection, intrusion, and surveillance technology
c.	Improve intelligence
d.	Provide funding for research on improving technology and policy
e.	National security improvements
f.	Development of intelligent devices and technologies for security and defense

Table 7.6 Risk Estimation Process for Intelligence Analysis

Step 1: Causative events
a. The terrorist leaders and supporters provided description and identified the routine pathways and locations of rail transportation system carrying nuclear bomb materials
b. Terrorists generated misleading events to divert US intelligence attention The terrorists created minor attacks on another infrastructure but did not cause any casualties on others such as the cyberspace The amateur terrorists created minor attacks on other parts of the state for media attention and intentionally got caught by authorities
c. Terrorist leaders and/or corrupt nations acquired nuclear bomb materials from the attack of rail transportations system
Step 2: Outcome
d. The terrorists are currently planning for high-profile attacks, improving their own intelligence, and gaining more financial support while the United States continues to exhaust its financial resources
Step 3: Exposure
e. The terrorists urgently developed WMD
f. The terrorists transported the weapons through underground tunnels on US borders
Step 4: Consequence
g. The terrorists achieved their ultimate mission
Step 5: Consequence value
h. Enhanced intelligence

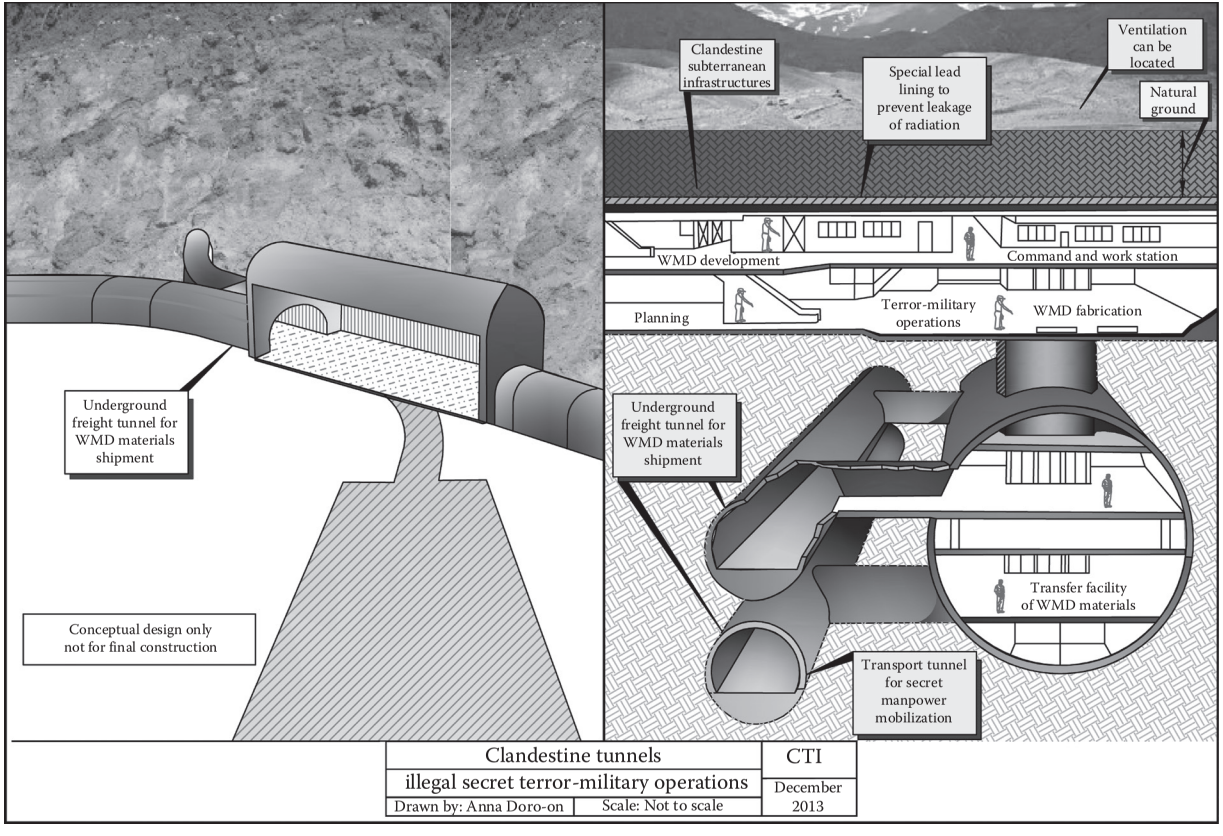
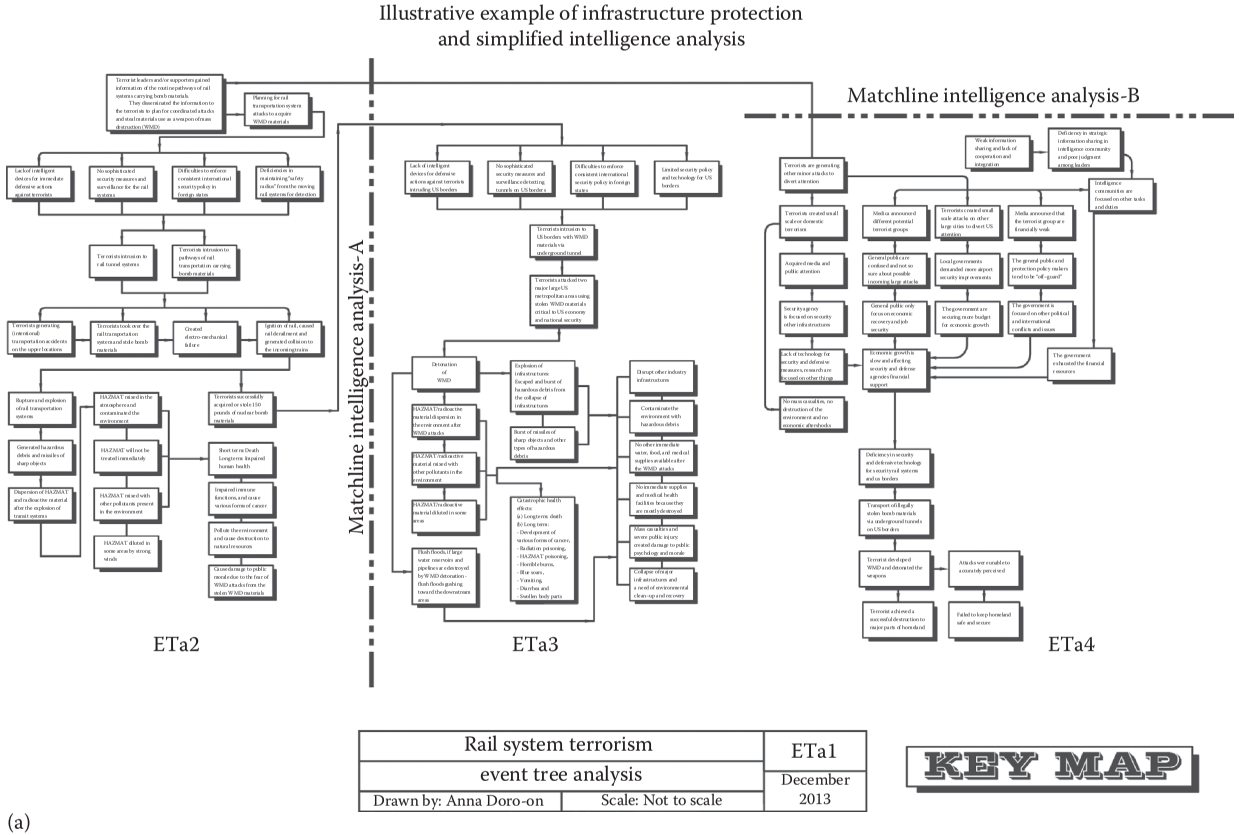


Figure 7.5 Clandestine tunnels for WMD productions and terror-military operations.



(a)

Figure 7.6 (a) The event tree analysis for terrorism on rail systems and basic intelligence analysis—key map.



Figure 7.6 (continued) (b) The event tree analysis for terrorism on rail systems and basic intelligence analysis.

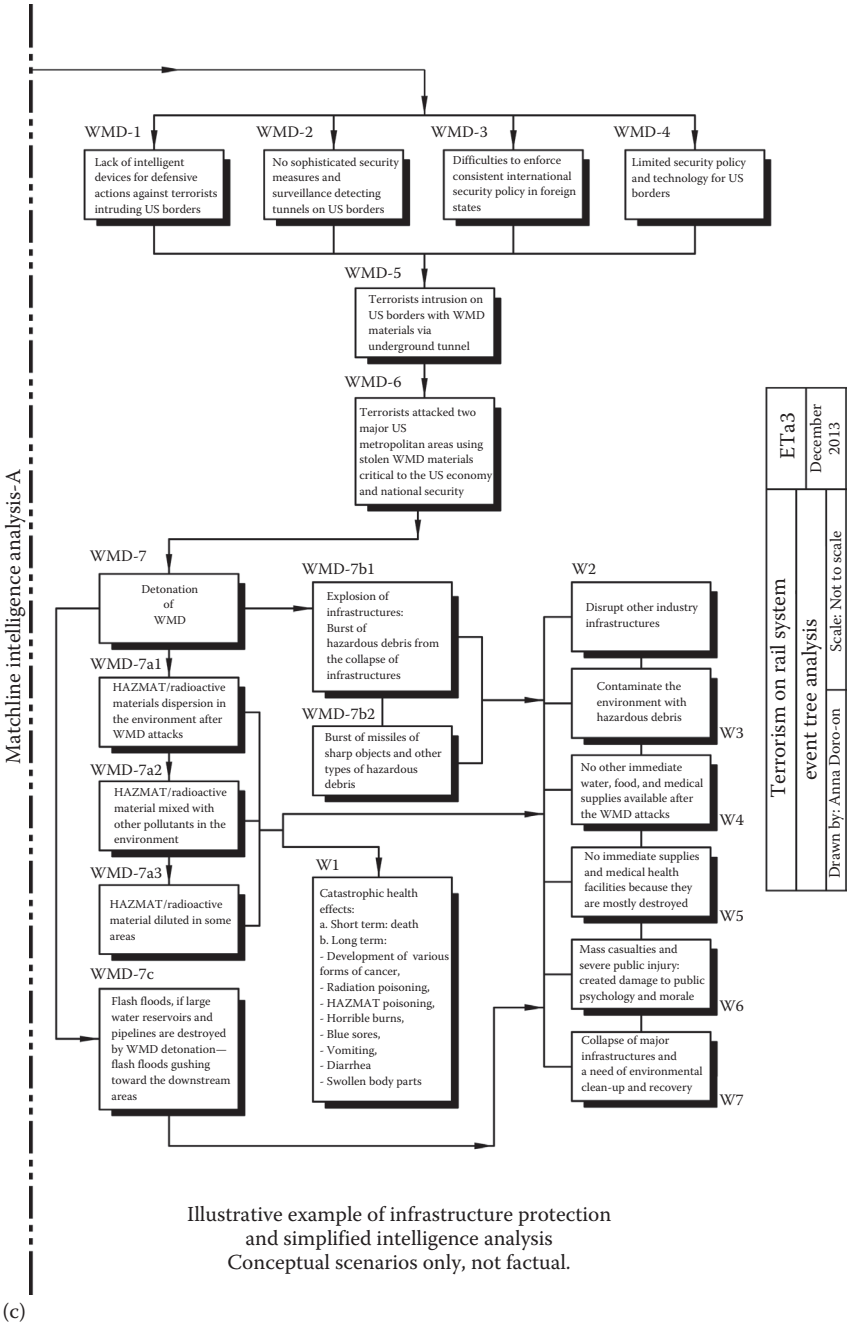
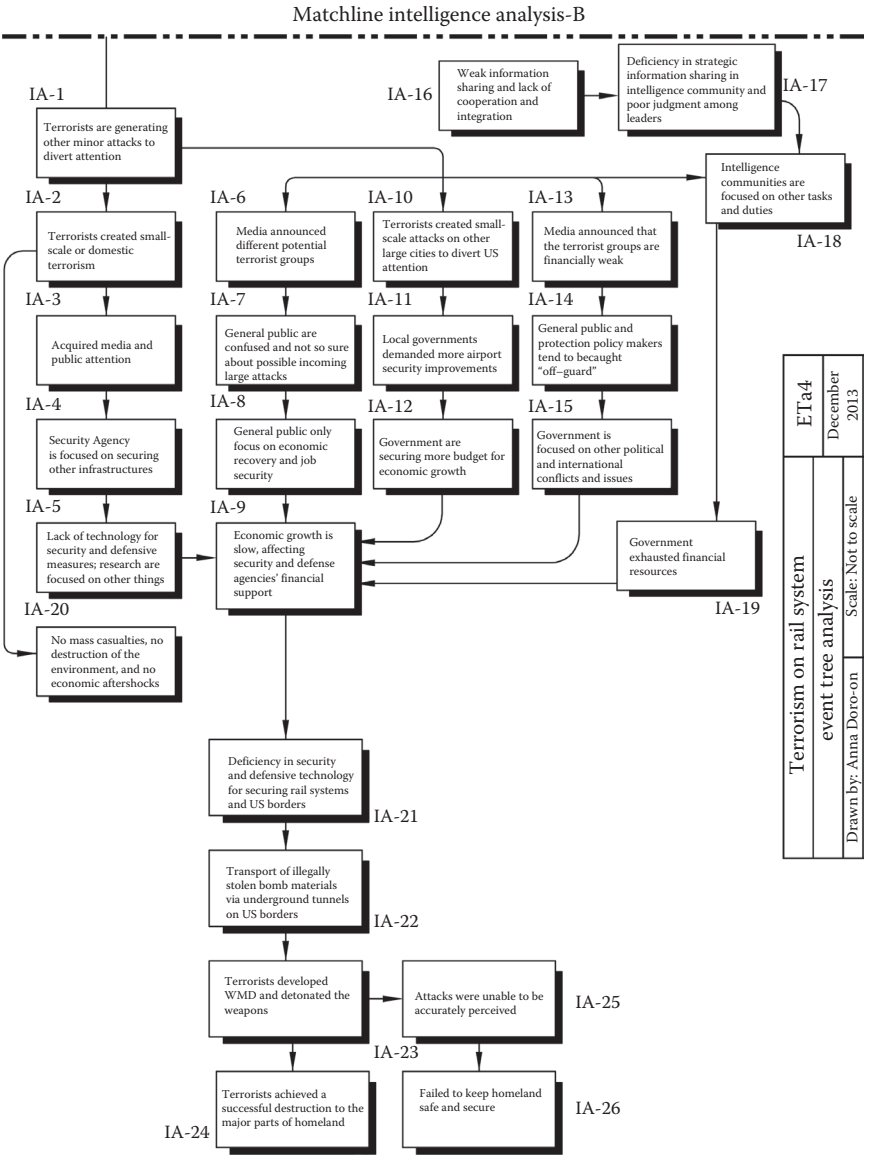


Figure 7.6 (continued) (c) The event tree analysis for terrorism on rail systems and basic intelligence analysis.



(d)

Figure 7.6 (continued) (d) The event tree analysis for terrorism on rail systems and basic intelligence analysis.

Table 7.7 Probability Scale Used for the Critical Infrastructure Analysis Risk Estimation Model

Probability Scale for Critical Infrastructure and Key Resources Protection Analysis		
Category	*Description*	*Probabilities in Decimal Description*
4	Very high (indicates that there are no effective policy or protective and defensive measures currently in place to deter, detect, delay, and respond to the threat)	0.90–1.00
	High (there are some policy and protective and defensive measures to deter, detect, delay, or respond to the asset but not a complete or effective application of these security strategies)	0.80–0.89
		0.71–0.79
3	Medium high	0.61–0.70
	Medium low (indicates that although there are some effective policy, protective, and defensive measures, there is no complete and effective application of these security strategies)	0.40–0.60
2	Low (indicates that there are effective protective and defensive measures in place; however, at least one weakness exists that an adversary would be able to defeat the countermeasure)	0.20–0.398
		0.10–0.198
1	Less likely—very low probability (indicates no credible evidence of capability)	0.05–0.099
		0.025–0.049
		<0.024

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2011.

7.7 Perspectives of Risk Acceptability in Strategic Intelligence Analysis

Incorporating quantitative psychology of risk considerations into tactical intelligence analysis is not simple. In the intelligence agencies and organizations, there are several concepts of risk. One standard method is to identify risk in terms of the

Table 7.8 Probability Scale Used for Intelligence Analysis Risk Estimation Model

Probability Scale for Intelligence Analysis		
Category	*Description*	*Probabilities in Decimal Description*
4	Very high (indicates that there are no effective strategies, or is business as usual, currently in place to accurately validate the information)	0.90–1.00
	High (there are some strategies and procedures to acknowledge the validity of the information but not an effective application of these strategies)	0.80–0.89
		0.71–0.79
3	Medium high (indicates that although there are some effective strategies and procedures, there is no effective application of these strategies)	0.61–0.70
	Medium low (indicates that there are effective strategies in place; however, at least one weakness exists that defeats the strategy to validate the accuracy of the information)	0.40–0.60
2	Low (indicates that there are effective strategies and sophisticated technologies but at least one information that is not totally clear)	0.20–0.398
		0.10–0.198
1	Very low probability (there are effective strategies and sophisticated technologies that validate the information being provided)	0.05–0.099
		0.025–0.049
		<0.024

Source: Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2011.

probability that some undesirable event with a negative consequence will occur. This is valid for the risk related to accidents (e.g., gas pipeline explosion). Intelligence formulation involving risk is to include most possible factors that will be influenced and should identify the consequences. The probabilities of occurrence can then be computed using a stochastic model to characterize the events, engagements, and the perceived risk intuitively. A salient technique to delineate the alternative outcomes that involve risk is the event tree analysis, as shown in Figure 7.6a through d.

Table 7.9 Risk Rates Based on Engineering Judgment of the Event Tree Analysis for Terrorism on Rail Systems and Basic Intelligence Analysis

Symbol	*Event Tree List of Events*	*Risk Rate*
RT-A1	Terrorist leaders and supporters gained information of the routine pathways of rail systems carrying bomb materials. They disseminated the information to the terrorists to plan for coordinated attacks and steal materials used as a weapons of mass destruction (WMD)	0.10
RT-A2	Planning for rail transportation system attacks to acquire WMD materials	0.20
RT-B1	No sophisticated security measures and surveillance for the rail systems	1.0
RT-B2	Difficulties in enforcing consistent international security policy in foreign states	0.20
RT-B3	Difficulties in enforcing consistent international security policy in foreign states	0.50
RT-B4	Deficiencies in maintaining "safety radius" from the moving rail systems for detection	1.0
RT-C1	Terrorists' intrusion in rail tunnel systems	0.50
RT-C2	Terrorists' intrusion into pathways of rail transportation carrying bomb materials	0.50
RT-Ca	Terrorists generating (intentional) transportation accidents further down the locations	0.50
RT-Cb	Terrorists took over rail transportation system and stole bomb materials	0.40
RT-Cc	Created electromechanical failure	0.40
RT-Cd	Ignition of rail caused rail derailment and generated collision to incoming passenger trains	0.80
RT-D	Rupture and explosion of rail transportation systems	0.95
RT-Da	Generated hazardous debris and missiles of sharp objects	0.95
RT-Db	Dispersion of HAZMAT and radioactive material after the explosion of transit systems	0.95
RT-De	HAZMAT mixed in the atmosphere and contaminated the environment	0.90

Table 7.9 (continued) Risk Rates Based on Engineering Judgment of the Event Tree Analysis for Terrorism on Rail Systems and Basic Intelligence Analysis

Symbol	*Event Tree List of Events*	*Risk Rate*
RT-Df	HAZMAT will not be treated immediately	0.90
RT-Dg	HAZMAT mixed with other pollutants present in the environment	0.90
RT-Dh	HAZMAT diluted in some areas by strong winds	1.0
RT-F	Terrorists successfully acquired or stole 150 lbs of nuclear bomb materials	0.50
RT-E1	Short term: death	0.75
	Long term: impaired human health	
RT-E1a	Impairs immune functions and cause various forms of cancer	0.75
RT-E1b	Pollute the environment and cause various forms of cancer	0.75
RT-E1c	Cause damage to public morale due to the fear of WMD attacks from the stolen WMD materials	0.95
WMD-1	Lack of intelligent devices for defensive actions against terrorists intruding US borders	1.0
WMD-2	No sophisticated security measures and surveillance detecting tunnels on US borders	0.50
WMD-3	Difficulties in enforcing consistent international security policy in foreign states	0.50
WMD-4	Limited security policy and technology for US borders	0.50
WMD-5	Terrorists' intrusion into US borders with WMD materials via underground tunnel	0.40
WMD-6	Terrorists attacked two major large US metropolitan areas using stolen WMD materials critical to US economy and national security	0.40
WMD-7	Detonation of WMD	0.80
WMD-7a1	HAZMAT/radioactive material dispersion in the environment after WMD attacks	0.90

(*continued*)

Table 7.9 (continued) Risk Rates Based on Engineering Judgment of the Event Tree Analysis for Terrorism on Rail Systems and Basic Intelligence Analysis

Symbol	*Event Tree List of Events*	*Risk Rate*
WMD-7a2	HAZMAT/radioactive material mixed with other pollutants in the environment	0.90
WMD-7a3	HAZMAT/radioactive material diluted in some areas	0.90
WMD-7c	Flush floods, if large water reservoirs and pipelines are destroyed by WMD detonation—flush floods gushing toward the downstream areas	0.05
WMD-7b1	Explosion of infrastructures: escape and burst of hazardous debris from the collapse of infrastructures	0.80
WMD-7b2	Burst of missiles of sharp objects and other types of hazardous debris	0.80
W1	Catastrophic health effects Short term: death Long term: development of various forms of cancer, radiation poisoning, HAZMAT poisoning, horrible burns, blue soars, vomiting, diarrhea, and swollen body parts	0.95
W2	Disrupt other industry infrastructures	0.95
W3	Contaminate the environment with hazardous debris	0.95
W4	No other immediate water, food, and medical supplies available after the WMD attacks	0.95
W5	No immediate supplies and medical health facilities because most are destroyed	0.95
W6	Mass casualties and severe public injury: create damage to public psychology and moral	0.95
W7	Collapse of major infrastructures	0.95
IA-1	Terrorists are generating other minor attacks to divert attention	0.10
IA-2	Terrorists create small-scale or domestic terrorism	0.10
IA-4	Acquired media and public attention	0.50
IA-5	Security agency is focused on securing other infrastructures	0.50
IA-6	Media announced different potential terrorist groups	0.10

Table 7.9 (continued) Risk Rates Based on Engineering Judgment of the Event Tree Analysis for Terrorism on Rail Systems and Basic Intelligence Analysis

Symbol	*Event Tree List of Events*	*Risk Rate*
IA-7	General public are confused and not so sure about possible incoming large attacks	0.60
IA-8	General public only focuses on economic recovery and job security	0.80
IA-9	Economic growth is slow and affecting security and defense agencies' financial support	0.30
IA-10	Terrorists created small-scale attacks on other large cities to divert US attention	0.10
IA-11	Local governments demanded more airport security improvements	0.90
IA-12	The government is securing larger budget for economic growth	0.60
IA-13	Media announced that the terrorist group is financially weak	0.50
IA-14	The general public and protection policy makers tend to be "off-guard"	0.30
IA-15	The government is focused on other political and international conflicts and issues	0.50
IA-16	Weak information sharing and lack of cooperation and integration	0.05
IA-17	Deficiency in strategic information dissemination in intelligence community and poor judgment among leaders	0.05
IA-18	Intelligence communities are focused on other tasks and duties and overlooked rail systems	0.10
IA-19	The government exhausted the financial resources	0.50
IA-20	No mass casualties, no destruction of the environment, and no economic aftershocks	0.80
IA-21	Deficiency in security and defensive technology for securing rail systems and US borders	0.50
IA-22	Transport of illegally stolen bomb materials via underground tunnels on US borders	0.50
IA-23	Terrorists developed WMD and detonated the weapons	0.40

(*continued*)

Table 7.9 (continued) Risk Rates Based on Engineering Judgment of the Event Tree Analysis for Terrorism on Rail Systems and Basic Intelligence Analysis

Symbol	*Event Tree List of Events*	*Risk Rate*
IA-24	Terrorists achieved successful destruction to major parts of homeland	0.80
IA-25	Attacks were unable to be accurately perceived	0.50
IA-26	Failed to keep homeland safe and secure	0.80

7.7.1 Risk Estimation and Risk Acceptability

Based on the event tree analysis for a terrorist attacks against the rail system for transshipment of bomb materials, as shown in Figure 7.4a, the comparison of risk estimation and risk acceptability is presented in Table 7.10. The detailed incremental risk acceptability quantifications and results are presented in Table 7.11. Finally, the comparison of strategic alternatives for US intelligence and rail system defense against terrorism is presented in Table 7.12.

US intelligence is the gist to all the effort for homeland and critical infrastructure protection and defense. The US IC (2008) and DHS (2008a,b) acknowledged and emphasized that improving the strategy and policy relating to the intelligence enterprise can be a lead toward enhancing the security of US critical infrastructures. However, intelligence is not the only critical element in maintaining the mission and goal for the protection of critical assets. Based on the analyses presented in Tables 7.10 through 7.12, to prevent the enemy from stealing nuclear materials during transshipments of classified materials, to deter the enemy from shipping WMD materials to homeland, and to terminate the enemy's actions, alternative 3 should be implemented to achieve acceptable risk from nuclear attack. There is currently, however, a very small probability that this would happen; however, this very small probability that it could occur is definitely compromising national security. Further discussion related to military operations and support will be elaborated in the following sections. Detailed risk assessments for pipelines, tunnels, underground rail, and transit systems are also demonstrated in the following sections.

7.8 Perspectives of Risk Acceptability Analysis for Pipelines, Tunnels, Underground Rail, and Transit Systems

This section presents detailed illustrations of the risk assessment and risk acceptability analysis based on the risk estimation models described in Chapter 5 (refer to Tables 7.13 through 7.22) for pipelines, tunnels, underground rail, and transit

Table 7.10 Risk Estimation and Risk Acceptability Analysis Comparison

Sl. No.	*Description*	*Risk Estimation*	*Risk Acceptability* $V(f) = \omega(p) \cdot v(x)$
1	Terrorists attacked and ignited rail system which carried nuclear weapon materials	1.6×10^{-4} (very high risk)	3.3×10^{-15} (very unacceptable risk)
2	Terrorists successfully acquired 150 lbs of stolen enriched uranium 235 (nuclear bomb material)	8.0×10^{-5} (high risk)	3.3×10^{-15} (very unacceptable risk)
3	Terrorists' intrusion into US borders via underground tunnel carrying stolen bomb material and used that to attack homeland	1.6×10^{-6} (high risk)	2.4×10^{-17} (very unacceptable risk)
4	Terrorist group allowed media to disseminate information that the terrorist group has no capability to acquire WMD and has no financial resources to mislead US public belief	5.0×10^{-5} (can pose very high risk if the intelligence community is not able to detect illegal intrusion into US borders with stolen bomb materials)	5.9×10^{-13} (very unacceptable risk)
5	Undetected transport of bomb materials on US border ready for detonation	1.5×10^{-6} (high risk)	9.8×10^{-17} (very unacceptable risk)
6	Terrorism act was unable to be accurately perceived	7.5×10^{-7} (high risk)	2.4×10^{-17} (very unacceptable risk)
7	Successful terrorism in one of the largest metropolitan areas	1.2×10^{-6} (high risk)	1.1×10^{-15} (very unacceptable risk)

Table 7.11 Risk Acceptability Analysis

Sl. No.	*Description*	*Risk Reference*	*Proportionality by Degree of Voluntarism*	*Derating*	*Controllability*	*Risk Acceptability* $V(f)=\omega(p)\cdot v(x)$
1	Terrorists attacked and ignited rail system which carried nuclear weapon materials	9.8×10^{-8} Man-originated catastrophic involuntary	0.09	0.000065	5.6×10^{-3}	3.3×10^{-15}
2	Terrorists successfully acquired 150 lbs of stolen enriched uranium 235 (nuclear bomb material)	9.8×10^{-8} Man-originated catastrophic involuntary	0.09	0.000065	5.6×10^{-3}	3.3×10^{-15}
3	Terrorists' intrusion into US borders via underground tunnel carrying stolen bomb material and used that to attack homeland	9.8×10^{-8} Man-originated catastrophic involuntary	0.09	0.000065	4.1×10^{-5}	2.4×10^{-17}

4	Terrorist group allowed media to disseminate information that the terrorist group has no capability to acquire WMD and has no financial resources to mislead US public belief	1.8×10^{-7} Man-originated catastrophic involuntary	0.09	0.0081	4.1×10^{-5}	5.9×10^{-13}
5	Undetected transport of bomb materials on US border ready for detonation	9.8×10^{-8} Man-originated catastrophic involuntary	0.09	0.000065	8.0×10^{-3}	9.8×10^{-17}
6	Terrorism act was unable to be accurately perceive	1.8×10^{-7} Man-triggered catastrophic involuntary	0.09	0.000065	4.1×10^{-5}	2.4×10^{-17}
7	Successful terrorism in one of the largest metropolitan areas	9.8×10^{-8} Man-originated catastrophic involuntary	0.09	0.000065	1.8×10^{-3}	1.1×10^{-15}

Table 7.12 Comparison of Strategic Alternatives for US Intelligence Improvements and Homeland Preventive Measures

Alternatives	*Risk Estimation*	*Risk Acceptability* $V(f)=\omega(p)\cdot v(x)$
1. Business as usual: Terrorism act was unable to be accurately perceive.	7.5×10^{-7} (high risk)	2.4×10^{-17} (very unacceptable risk)
2. Implement enhanced intelligence enterprise plan: utilize intuitive judgments in terms of intelligence analysis and effective intelligence information sharing for homeland and critical infrastructure protection. Currently, no intelligent devices to detect, deter, and terminate/capture the adversary.	6.2×10^{-4} (high risk) (Even though there are effective intelligence enterprise plans, utilizing intuitive judgments, intelligence processes, and effective but not defensive systems, there is a high probability for terrorists to gain stolen bomb materials and transport them to homeland illegally)	5.0×10^{-11} (very unacceptable risk)

3. Implement the following: a. Enhanced intelligence enterprise plan (Figure 7.8). b. Military support to homeland and critical infrastructure protection. c. Practice intuitive judgments in policy making and decision making in terms of homeland and critical infrastructure protection. d. Develop not only preventive measures but also "defensive" systems to deter, detect, and terminate/capture the enemy. Should also implement special technologies such as intelligent devices with designed safety—detection distances. e. Develop safety easement or encroachment from a critical infrastructure in conjunction with preventive and defensive approaches.	3.1×10^{-17} (very low risk)	9.0×10^{-9} (acceptable risk)

Table 7.13 Process of Risk Estimation for Pipelines, Tunnels, Rail, and Transit Systems; Step 1: Causative Events

a.	Terrorists' intrusion into oil and gas pipelines vicinities
b.	Terrorists' intrusion into underground freight transportation through pipelines, *cargo cap*, and *maglev* (Figures 7.16 and 7.18)
c.	Terrorists' intrusion into tubular rails (Figures 7.10 and 7.11)
d.	Terrorists' intrusion into major stations of underground high-speed mass transit
e.	Terrorists' intrusion into tunnel systems near populated/urban areas (e.g., road tunnels, rails, underwater/immersed tunnels, and drainage tunnel)
f.	Terrorists' intrusion into aqueducts (Figures 7.13 and 7.14)

Table 7.14 Process of Risk Estimation for Pipelines, Tunnels, Rail, and Transit Systems; Step 2: Outcome

a.	Placing of explosive devices at tunnel surfaces and outlets
b.	Placing of WMD in *tubular rails* and *maglev* operating in overpopulated areas or within large metropolitan areas
c.	Freight transportation pipeline rupture
d.	Using explosive devices to severely rupture oil and gas pipelines
e.	Destruction of aqueduct structures by explosive devices
f.	Placing chemical threats and explosive devices in tunnel systems
g.	Ignition of flammable material to freight system or cargo caps
h.	Generate rail derailment and collision
i.	Generate electromechanical failure and cyber-controller system failure

Table 7.15 Process of Risk Estimation for Pipelines, Tunnels, Rail, and Transit Systems; Step 3: Exposure

a.	Chemical threats dispersion in the environment after the explosion of transit systems (*i.e., maglev, and tubular rails*): i. Chemical threats mixed in the atmosphere and the environment ii. Chemicals will not be treated easily iii. Chemicals mixed with other pollutants present in the environment iv. Chemicals diluted in some areas by strong winds
b.	The release of HAZMAT in the environment after oil and gas pipelines rupture: i. HAZMAT contaminated the water bodies and soils of the surrounding environment after explosion ii. HAZMAT will not be treated immediately
c.	Explosions of transit systems (*i.e., maglev and tubular rails*) created by explosive devices i. Derailment and rupture of maglev and tubular rails ii. Missiles in flight from transit/rail system burst iii. Generate flash fires and fireballs iv. Dust and fragment explosions
d.	Flush flood after explosion of aqueducts: i. Floodwater from aqueducts destroyed the surrounding environment
e.	Explosions of tunnel systems due to rail systems collision and release of flammable liquids: i. Generation of debris and environmental contamination ii. Generation of flammable gas and liquid
f.	Rupture of underwater tunnels: i. Flush flood in underwater tunnels affecting the adjacent areas
g.	Rupture of rails and freights after strong collisions: i. Flash and pool fires during rail system disasters

Table 7.16 Process of Risk Estimation for Pipelines, Tunnels, Rail, and Transit Systems; Step 4: Consequence

a.	Catastrophic health effects i. Short-term effect: Death ii. Long-term effects: Impaired human health (impaired immune functions, cause various cancers, and radiation poisoning)
b.	Disrupt downstream commercial agriculture and industry infrastructure due to aqueduct destruction: i. Flood and contaminate the environment ii. No other immediate water supply available after the attack
c.	Injury to the environment due to the release of missiles and debris
d.	Result in economic distress due to the tremendous need for reconstruction of infrastructures and environmental remediation
e.	Cause damage to public morale and confidence
f.	Number of casualties and severe injuries after bursting of missiles
g.	Mass casualties
h.	Pollute the environment and cause destruction of natural resources dependent on clean environment (after the release of toxic substance)
i.	Collapse of key transportation and freight systems infrastructures
j.	Result in economic distress due to the need for emergency response and recovery after damaging oil and gas pipelines
k.	Result in economic distress due to the need for reconstruction and recovery after damaging rail tunnel systems

Table 7.17 Process of Risk Estimation for Pipelines, Tunnels, Rail, and Transit Systems; Step 5: Consequence Values

a.	Protection and security policy revision
b.	Provide detection, intrusion, and surveillance technology
c.	Improve intelligence
d.	Provide funding for research on improving technology and policy
e.	National security improvements
f.	Development of intelligent devices and technologies for security and defense approaches

Table 7.18 Process of Risk Estimation for Clandestine Tunnels and Transshipment of WMD Materials; Step 1: Causative Events

a.	Terrorists/rebellious nations constructed secret tunnels near overpopulated (metropolitan) areas.
b.	Terrorist/rebellious nations constructed secret infrastructures near or adjacent to underground freight transportation through pipelines and *maglev* trains to aid their manpower mobilization and terror operations and use those as a disguise system.
c.	Terrorists/rebellious nations built friendly relationships with other corrupt nations.
d.	Terrorists/rebellious nations secretly negotiated with other corrupt organizations/nations to acquire WMD materials, manpower mobilization, and hidden transport of WMD materials. They successfully developed powerful WMD and its components without being interrupted during fabrication.
e.	Terrorists/rebellious nations installed cover-up systems to hide illegal operations.
f.	Terrorists/rebellious nations constructed cross-border tunnels with other corrupt organizations for WMD materials and manpower transshipments.
g.	Terrorists/rebellious nations constructed "escape" infrastructures to protect their terrorism and devious leaders after the terror attacks.

Table 7.19 Process of Risk Estimation for Clandestine Tunnels and Transshipment of WMD Materials; Step 2: Outcome

a.	Preparing terror-military operations against homeland, allies, and friendly nations
b.	Preparing security and defense systems for a successful launch of terror-military operations and WMD attacks
c.	Preparing effective secret WMD launch sites for attacks
d.	Preparing intrusion and attack positions

Table 7.20 Process of Risk Estimation for Clandestine Tunnels and Transshipment of WMD Materials; Step 3: Exposure

a.	Chemical threats/radioactive material dispersion in the environment after the WMD attacks: i. Chemical threats/radioactive material mixed in the atmosphere and the environment ii. Chemical threats/radioactive material will not be treated immediately iii. Chemical threats/radioactive material diluted in some areas via strong winds
b.	Explosion of infrastructures after the attacks: i. Escape and burst of hazardous debris and gas from the collapse of infrastructures contaminated the surrounding environment ii. Hazardous debris, missiles, and gas will not be treated immediately
c.	Flush floods if large water reservoirs and pipelines are destroyed by WMD explosion: i. Flush floods gushing toward the downstream areas
d.	Detonation of WMD: i. Lethal energy, radiant heat, and shock waves released ii. Abrupt flash and pool fires and jet flames released to the environment iii. Flash burns

systems including clandestine tunnels for WMD production (illustrated in Figures 7.7, 7.8, 7.10, 7.11, 7.13, 7.14, 7.16, 7.18 and 7.20). The event tree analyses are presented in Figures 7.9, 7.12, 7.15, 7.17, 7.19, and 7.21. The risk rates for the event tree analyses are provided in Tables 7.23 through 7.28.

The analyses presented in Tables 7.29 through 7.31 have a similar implication as the analyses presented in the previous Tables 7.10 through 7.12, that alternative 2 would provide the most effective result for the protection of critical assets. One requisite to detect illegal clandestine subterranean infrastructure is to determine the vents and/or outlets; intelligent technologies can be utilized to gain validity of the existence of clandestine tunnels in certain locations to mitigate national and international security risks. Chapter 8 presents preventive measures for pipelines, tunnels, underground rail, and transit systems. The following sections discuss the understanding of military operations and the importance of military capabilities and limitations to support homeland security.

Table 7.21 Process of Risk Estimation for Clandestine Tunnels and Transshipment of WMD Materials; Step 4: Consequence

a.	Catastrophic health effects: i. Short-term effect: death ii. Long-term effects: impaired human health such as the development of various cancers, radiation poisoning, horrible burns, and untreatable *disease X* (*emergence of blue soars on body parts, vomiting, bleeding, diarrhea, and swollen body parts*)
b.	Disrupt all industry infrastructures after WMD attacks: i. Contaminate the environment ii. No other immediate water, food, and medical supplies available after the WMD attacks
c.	Destruction and injury to the environment due to the release of radioactive material, other HAZMAT, and debris
d.	Result in economic distress due to the tremendous requirement for reconstruction of infrastructures, environmental remediation, recovery, and emergency medical supplies
e.	Cause damage to public psychology, morale, and confidence
f.	No other immediate medical supplies and no immediate medical health facilities available because they are mostly destroyed after WMD attacks
g.	Mass casualties
h.	Destruction of preserved resources
i.	Collapse of major infrastructures critical to national economy and public safety

Table 7.22 Process of Risk Estimation for Clandestine Tunnels and Transshipment of WMD Materials; Step 5: Consequence Values

a.	Protection and security policy revision (national and international). Enhance international collaborations
b.	Development of intelligent devices and technologies to mitigate illegal operations
c.	Provide funding for research on improving technology and policy. Improve decision-making process in choosing research and technological projects
d.	Incorporate and practice of intuitive judgments and sound predictions to stakeholders, decision makers, analysts, and engineers
e.	Improve intelligence

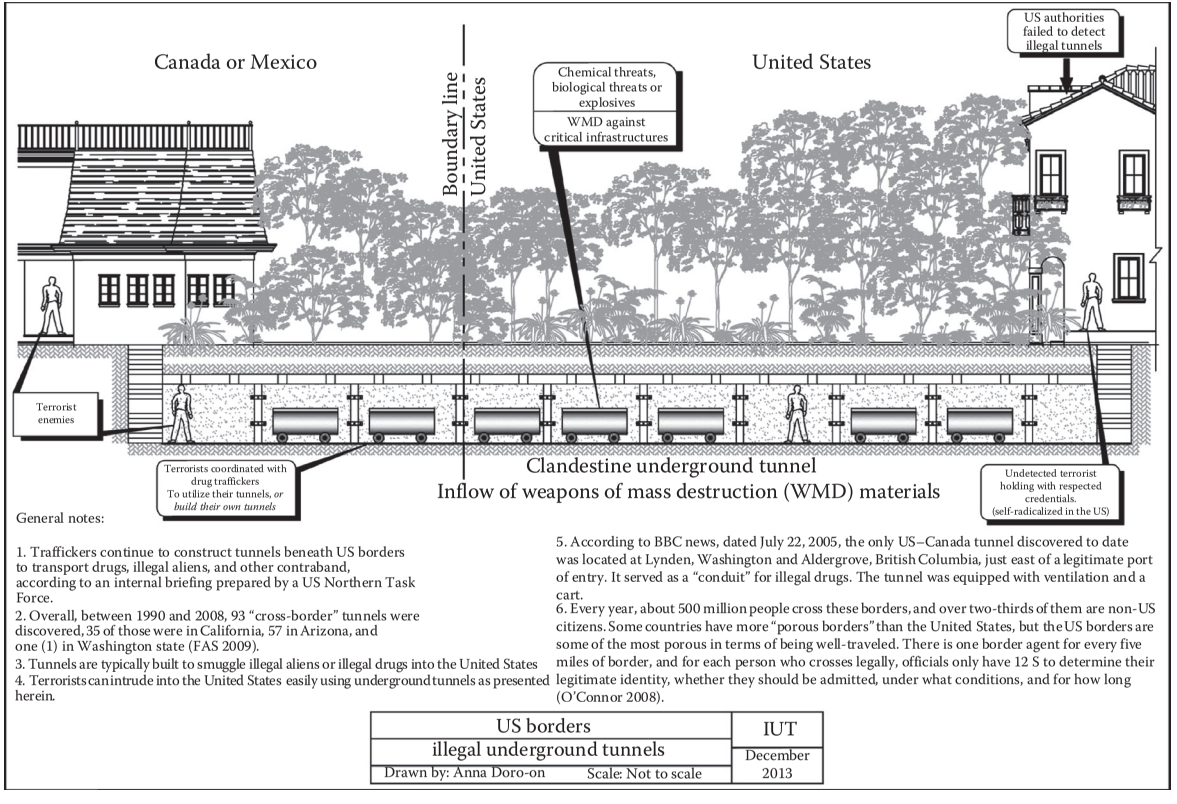


Figure 7.7 Clandestine tunnels on US borders. (From Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2011.)

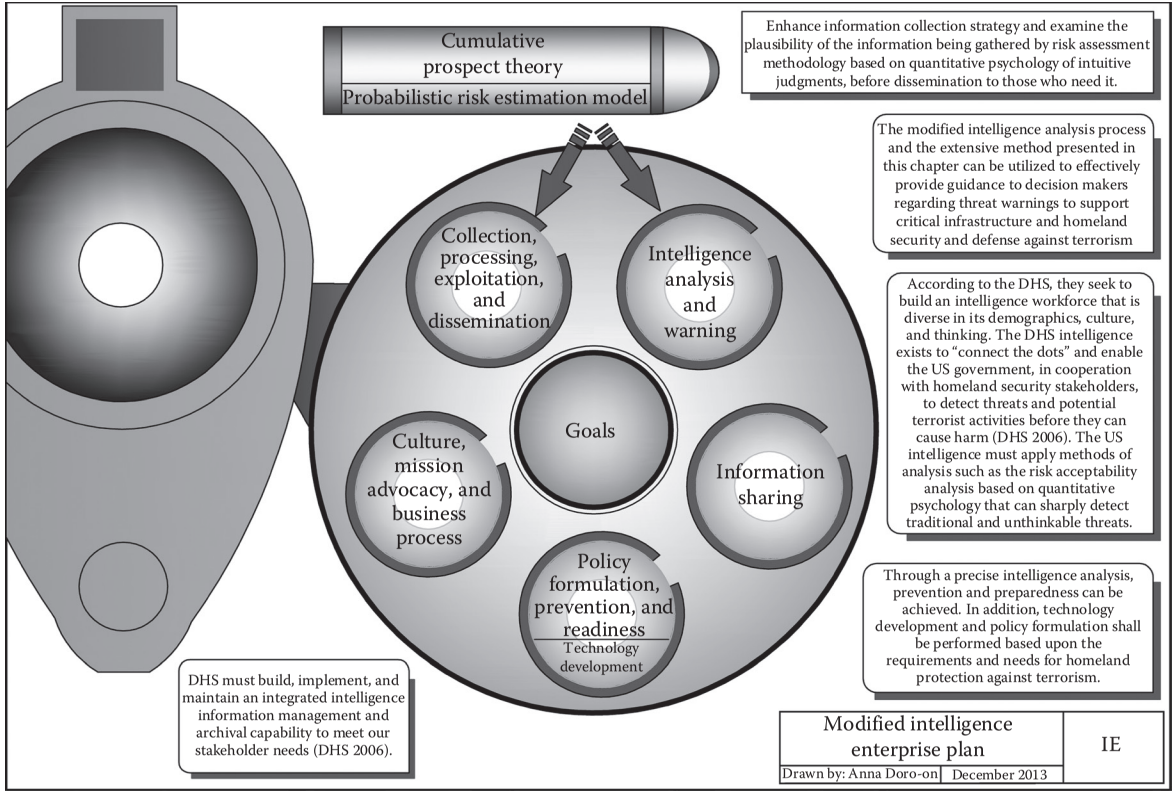


Figure 7.8 Modified intelligence enterprise plan for critical infrastructure and homeland security. (From Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2011.)

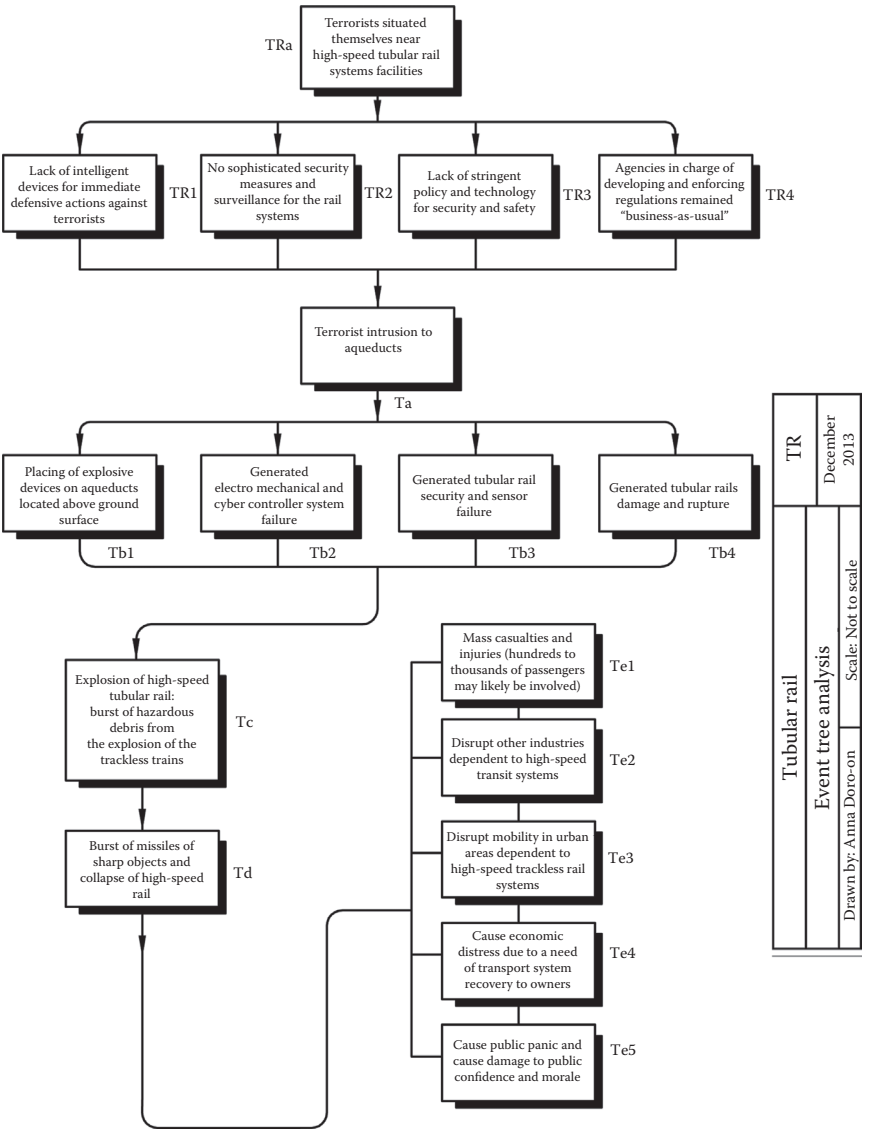


Figure 7.9 The event tree analysis for terrorism on tubular rails.

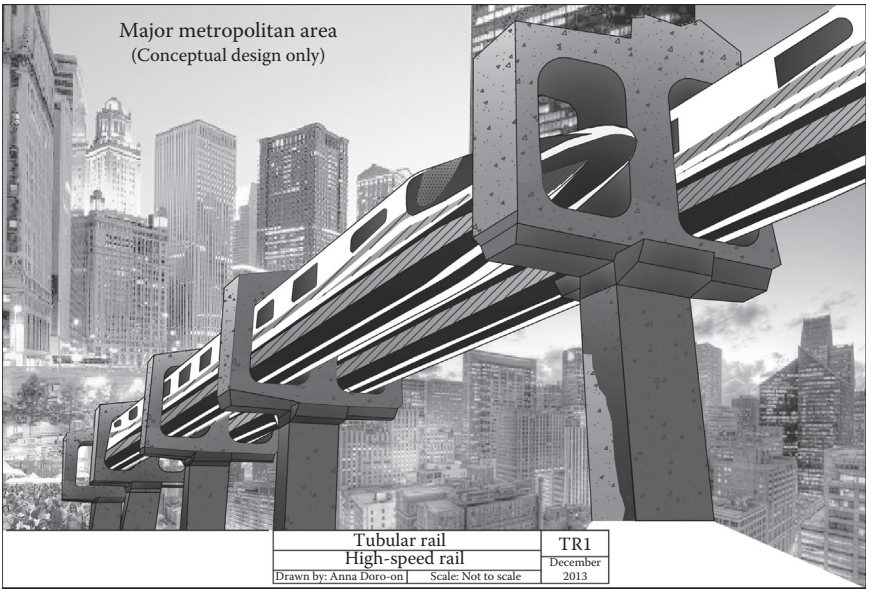


Figure 7.10 Tubular rail trackless train technology.

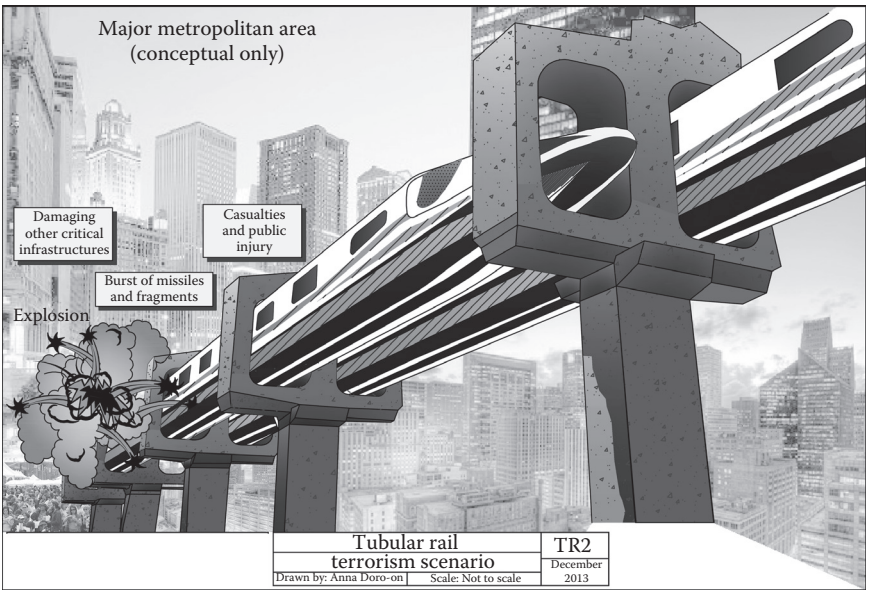


Figure 7.11 Tubular rail terrorism scenario.

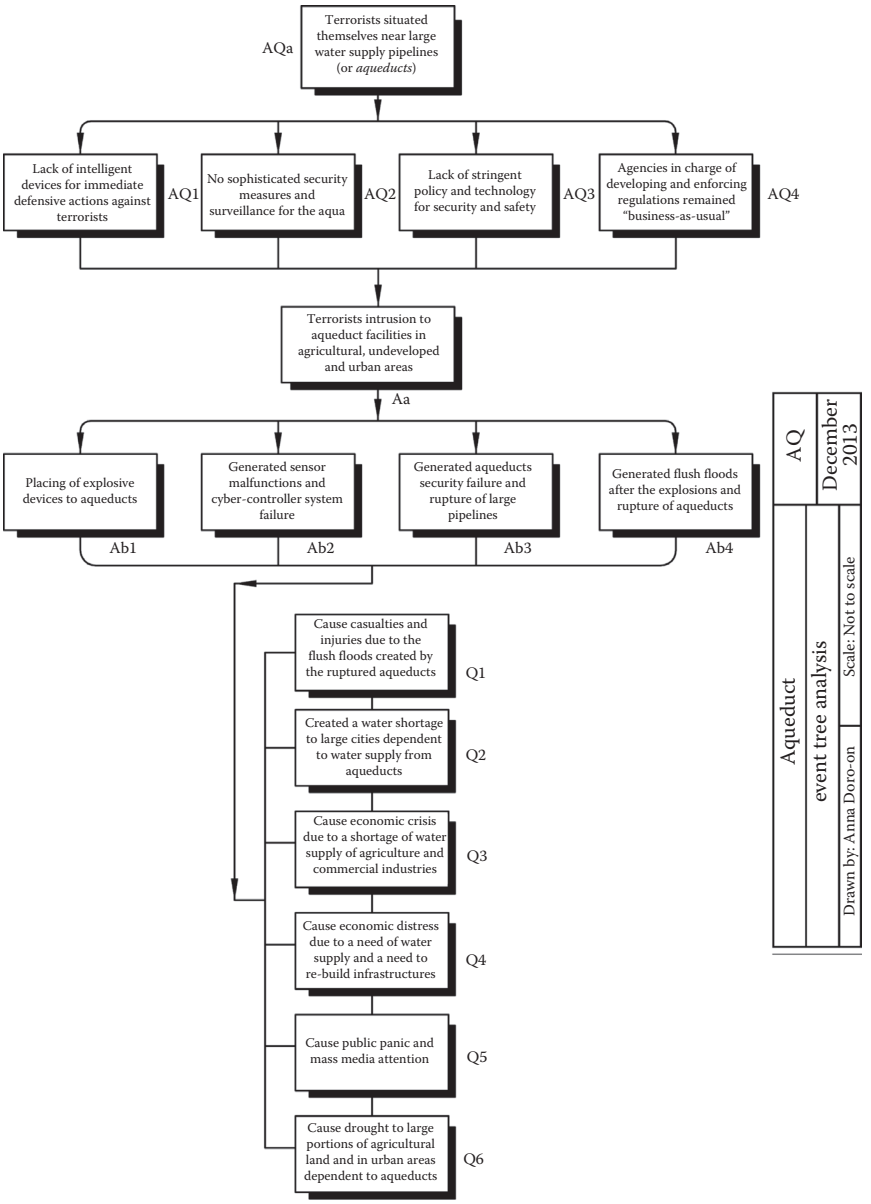


Figure 7.12 The event tree analysis for terrorism on aqueducts.

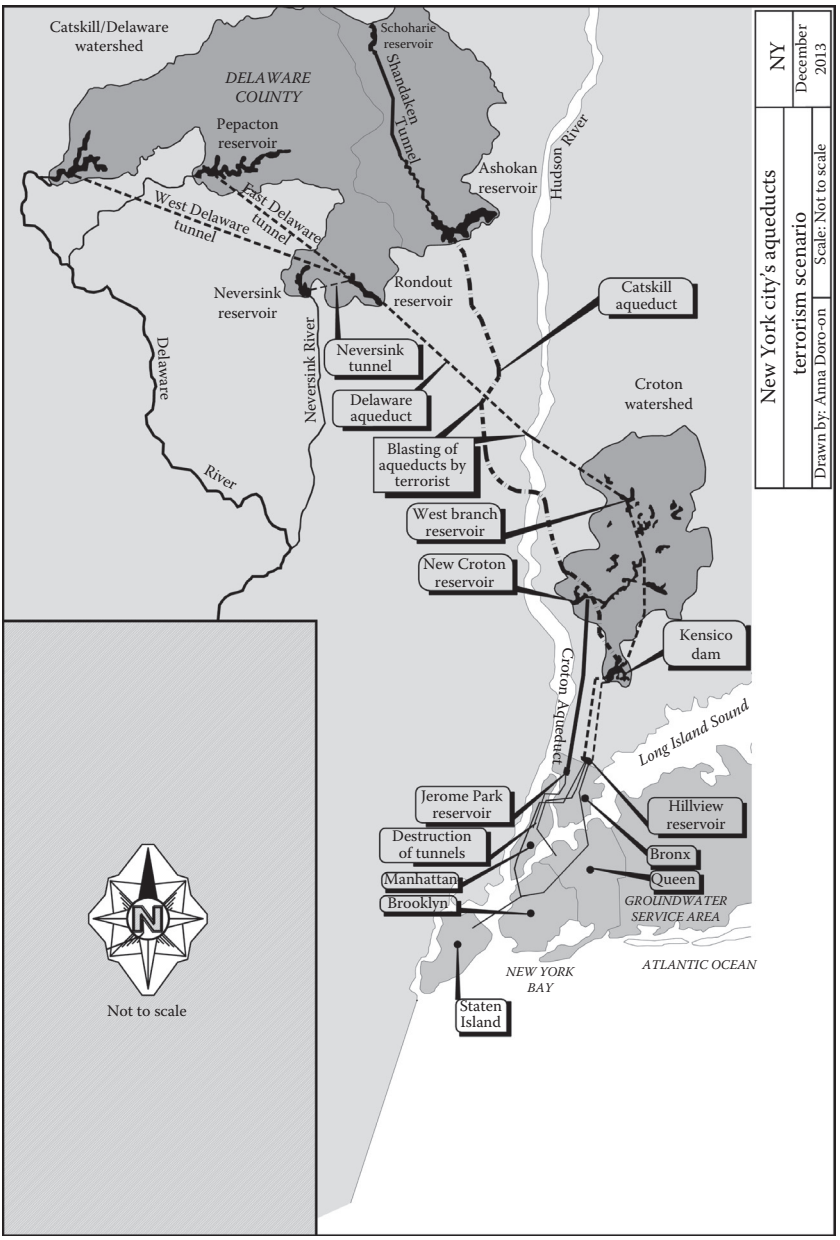


Figure 7.13 Aqueducts in New York. (From Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2011.)

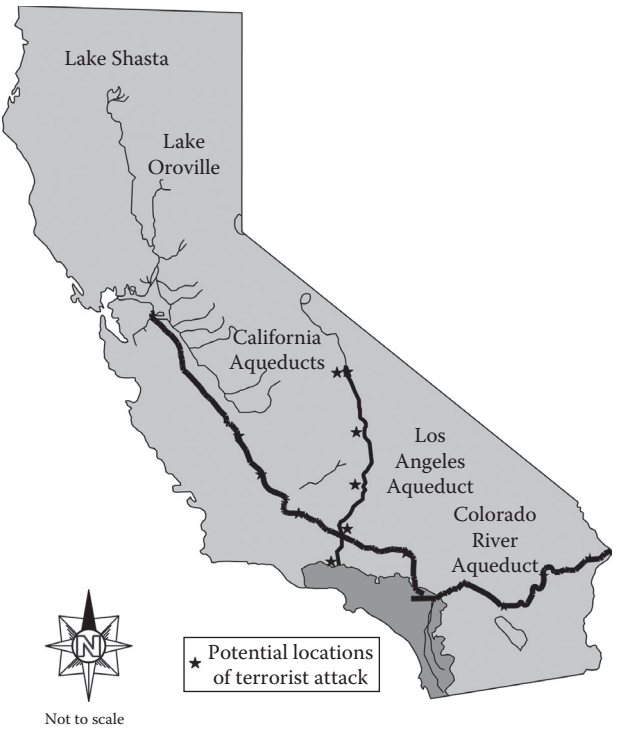


Figure 7.14 Aqueducts in California. (From Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2011.)

7.9 Military Intuitive Judgment and Decision-Making Process

The main objective of a government is to ensure abundance, freedom, economic growth, and most of all, maintaining national security. The laws of the State execute national policies and work an agreement with other States to execute international policies effectively. If there is any disagreement or opposition of policies with one another (e.g., one State to the other State), a peaceful settlement is offered. If none of those settlement methods or diplomatic measures being offered is acceptable to either or both States, one State will impose a stronger degree of measures against the rebellious State in the form of political, psychological, and economic pressure and/or use of *armed forces* which can include the imposition of *war*. Whether war is immoral or not, warfare is sometimes the only method to promote and defend a nation, allies, and friends' freedom, interests, and security. The main purpose of the armed forces is to begin by imposing *friendly forces* (does not require the use of

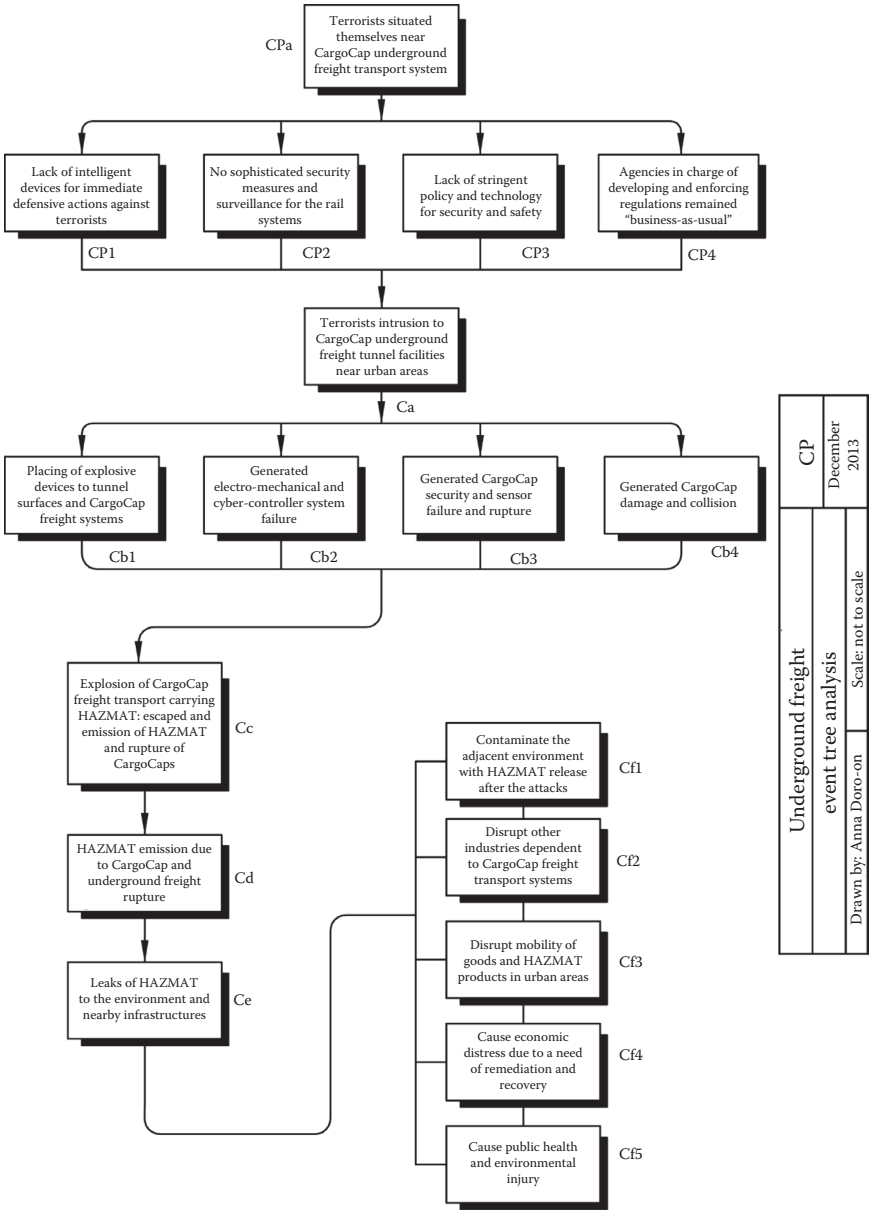


Figure 7.15 The event tree analysis for terrorism on CargoCap and other underground freight transportation through pipelines.

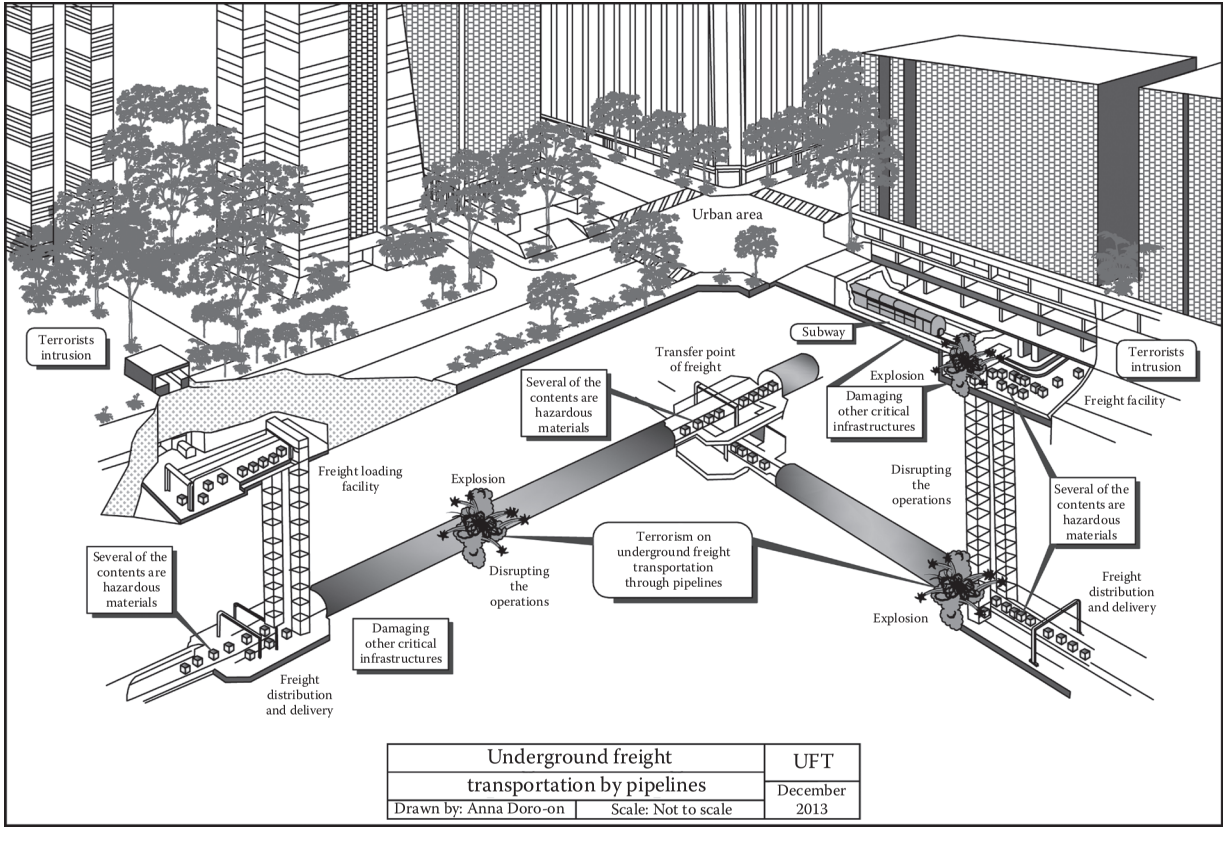


Figure 7.16 Underground freight transportation through pipelines.

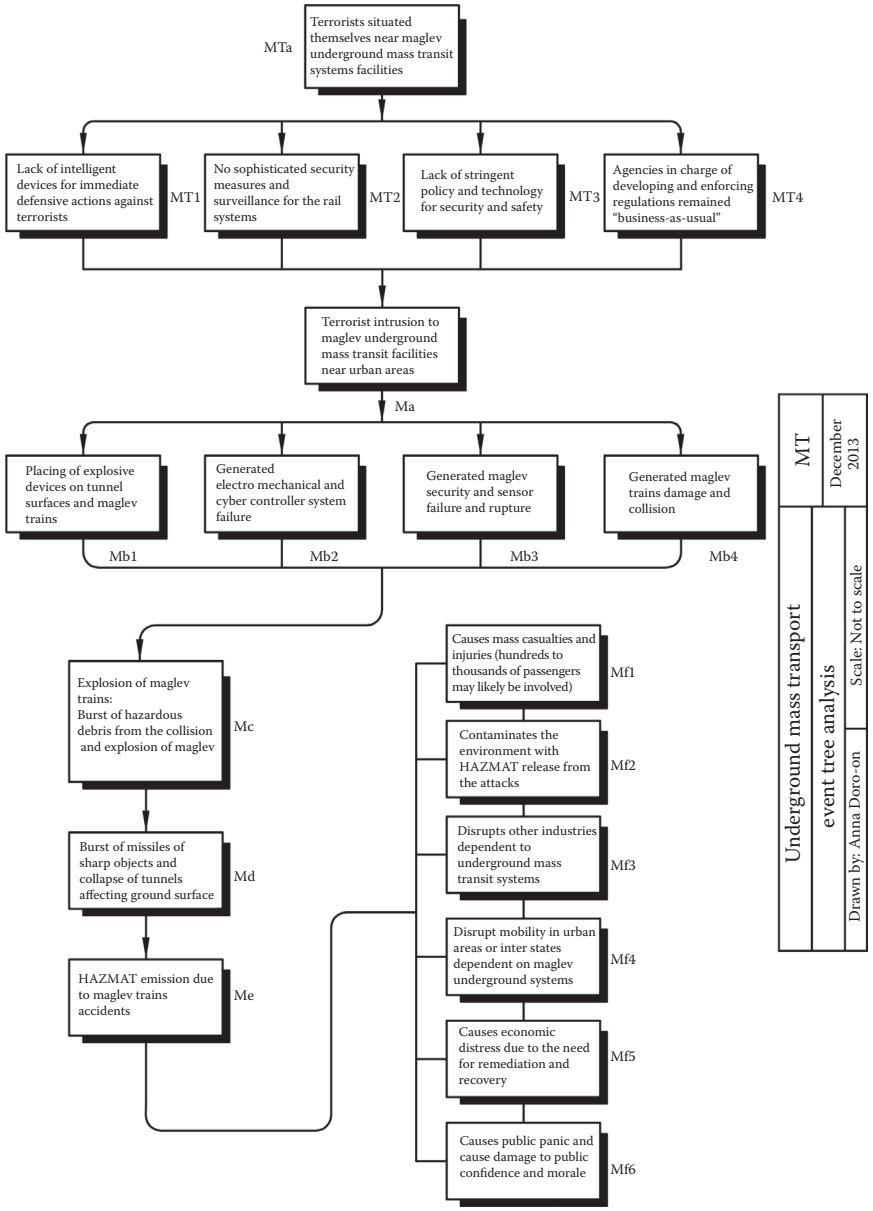


Figure 7.17 The event tree analysis for terrorism on underground magnetic levitation rapid transportation systems.

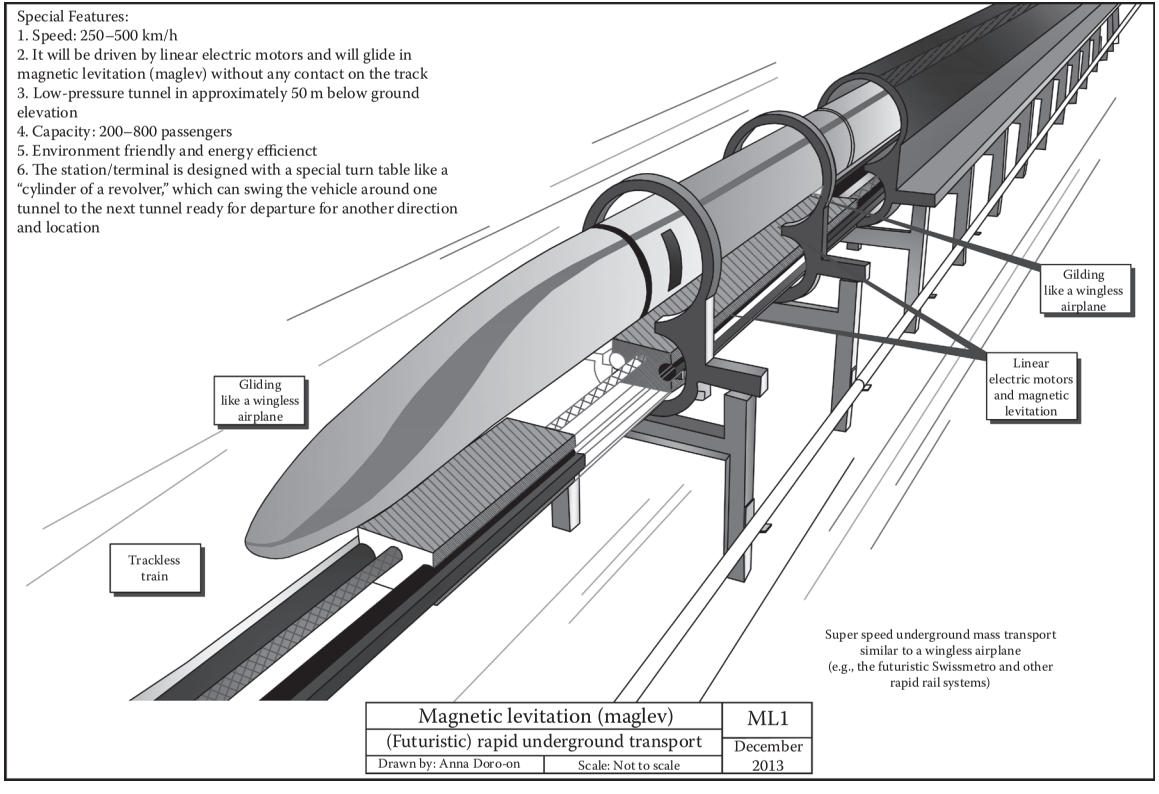


Figure 7.18 Example of magnetic levitation train.

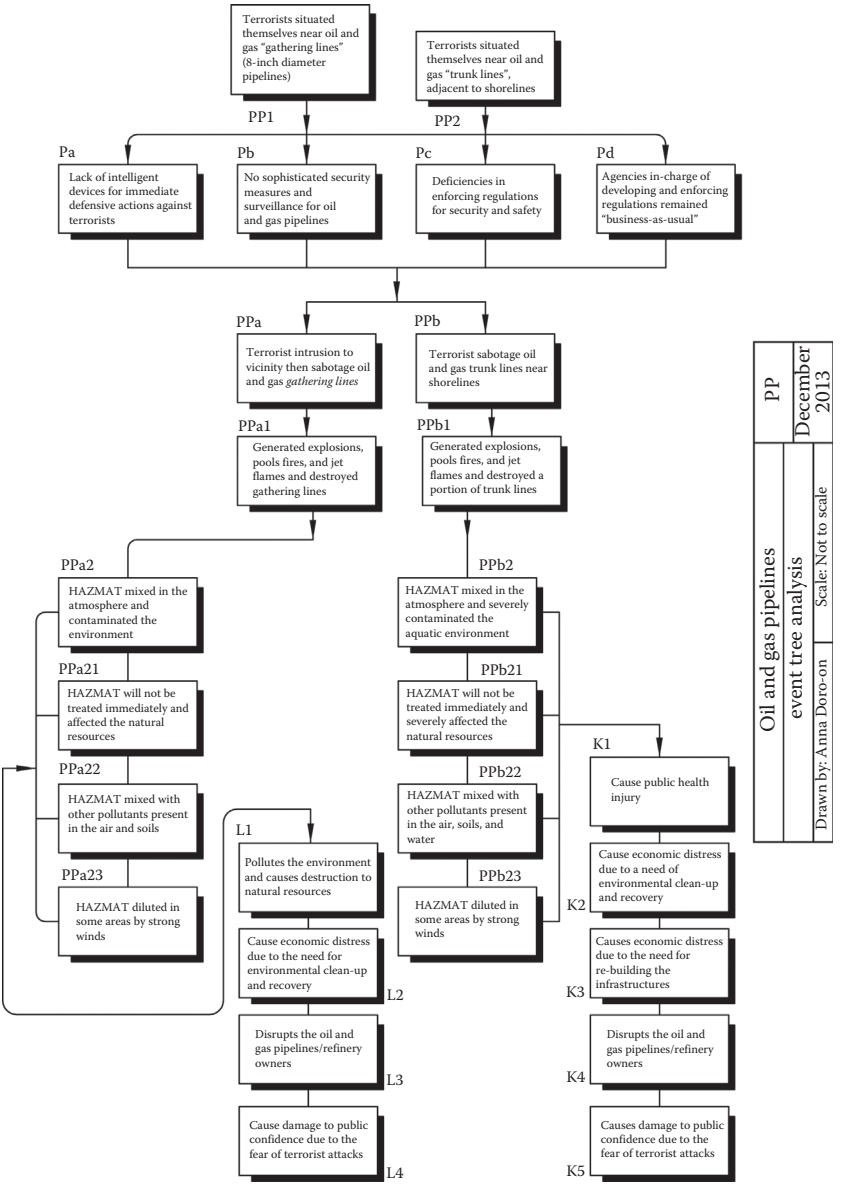


Figure 7.19 The event tree analysis for terrorism on oil and gas pipelines.

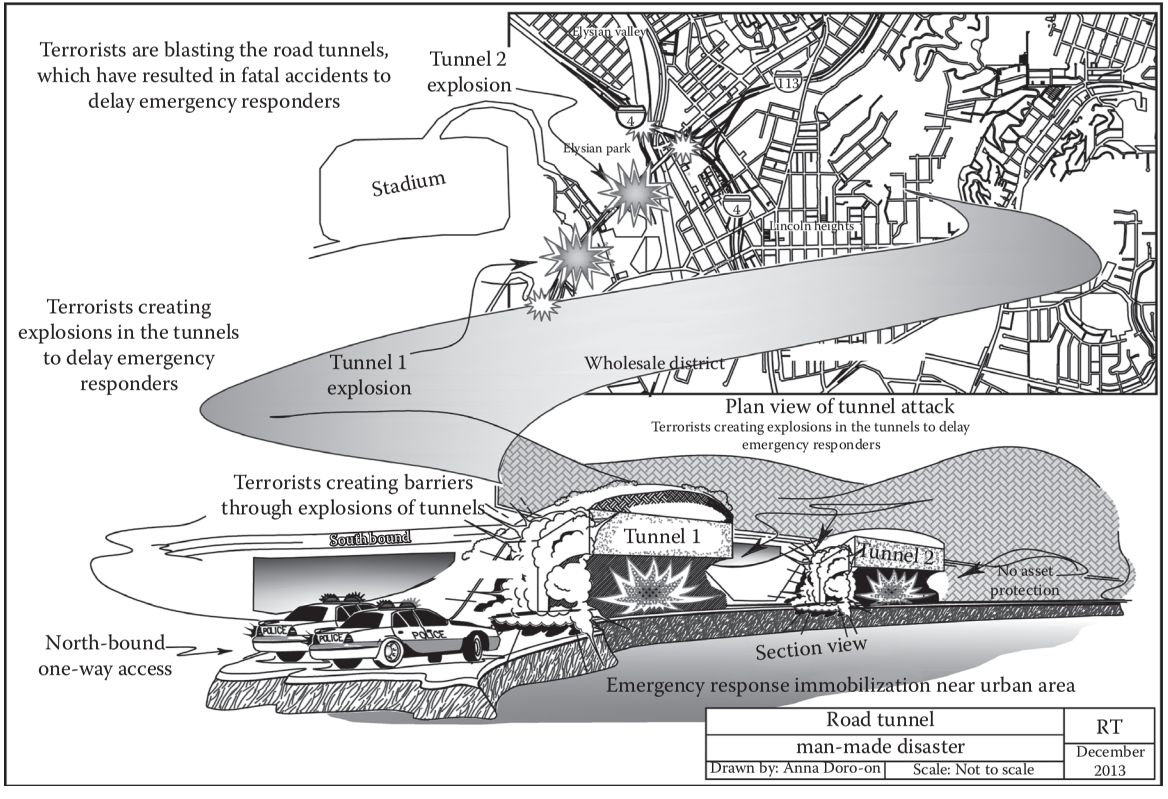
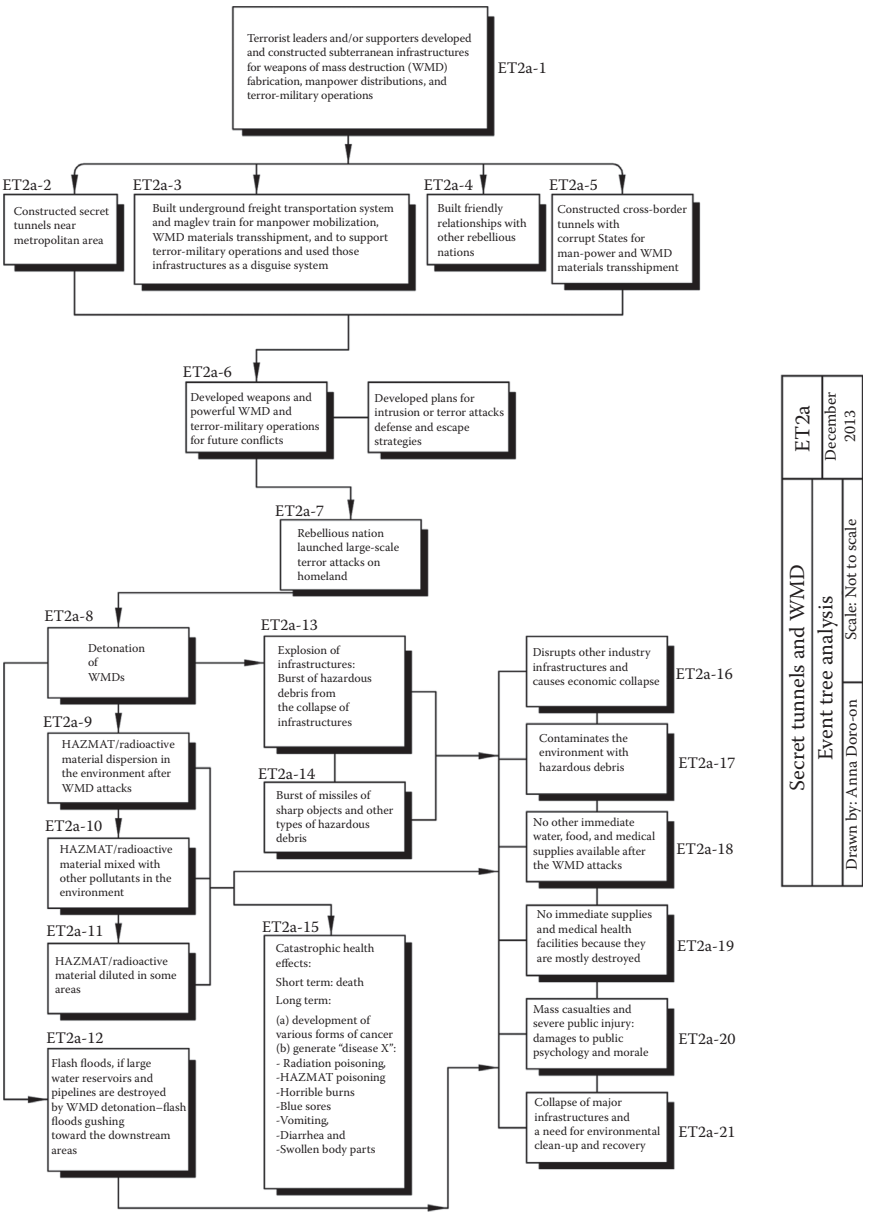


Figure 7.20 Road tunnel explosion. (From Doro-on, A., *Risk Assessment for Water Infrastructure Safety and Security*, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2011.)



Conceptual scenarios only, not factual.

Figure 7.21 The event tree analysis for the risk of secret tunnels and WMD.

Table 7.23 Risk Rates Based on Engineering Judgment of the Event Tree Analysis for Tubular Rail Trackless Train Technology

Symbol	*Event Tree List of Events*	*Risk Rate*
TRa	Terrorists situated themselves near high-speed tubular rail system facility	0.60
TR1	Lack of intelligent devices for immediate defensive actions against terrorists	1.0
TR2	No sophisticated security measures and surveillance for the rail systems	0.50
TR3	Lack of stringent policy and technology for security and safety	0.30
TR4	Agencies in charge of developing and enforcing regulations remained "business-as-usual"	0.20
Ta	Terrorists' intrusion into high-speed tubular rail and high-mass transit facilities near urban areas	0.60
Tb1	Placing of explosive devices to high-speed tubular rail technology	0.40
Tb2	Generated electromechanical and cyber-controller system failure	0.10
Tb3	Generated tubular rail security and sensor failure	0.10
Tb4	Generated tubular rail damage and rupture	0.40
Tc	Explosion of high-speed tubular rail: bust of hazardous debris from the explosion of the trackless trains	0.90
Td	Burst of missiles of sharp objects and collapse of high-speed rail	0.90
Te1	Mass casualties (hundreds to thousands of passengers may likely be involved)	0.95
Te2	Disrupt other industries dependent on high-speed transit systems	0.40
Te3	Disrupt mobility in urban areas dependent on high-speed rail systems	0.40
Te4	Cause economic distress due to a need of transport system	0.40
Te5	Cause public panic and cause damage to public confidence and morale	0.95

Table 7.24 Risk Rates Based on Engineering Judgment of the Event Tree Analysis for Aqueducts

Symbol	*Event Tree List of Events*	*Risk Rate*
AQa	Terrorists situated themselves near large water supply pipelines (or aqueducts)	0.75
AQ1	Lack of intelligent devices for immediate defensive actions against terrorists	1.0
AQ2	No sophisticated security measures and surveillance for the aqueducts	0.60
AQ3	Lack of stringent policy and technology for security and safety	0.30
AQ4	Agencies in charge of developing and enforcing regulations remained "business-as-usual"	0.60
Aa	Terrorists' intrusion into aqueducts facilities near agricultural land, undeveloped and urban areas	0.80
Ab1	Placing of explosive devices in aqueducts	0.40
Ab2	Generated sensor malfunctions and cyber-controller system	0.05
Ab3	Generated aqueducts security failure and rupture	0.80
Ab4	Generated flush floods after the explosions and rupture of aqueducts	0.50
Q1	Caused casualties and injuries due to the flush floods created by the ruptured aqueducts	0.40
Q2	Created a water shortage to large cities dependent on water supply from aqueducts	0.95
Q3	Caused economic crisis due to a shortage of water supply from aqueducts	0.95
Q4	Caused economic distress due to a need of water supply and a need to rebuild infrastructures	0.95
Q5	Caused public panic and mass media attention	0.95
Q6	Caused drought to large portions of agricultural land and to urban areas dependent on aqueducts	0.90

Table 7.25 Risk Rates Based on Engineering Judgment of the Event Tree Analysis for CargoCap

Symbol	*Event Tree List of Events*	*Risk Rate*
CPa	Terrorists situated themselves near CargoCap underground freight transportation system	0.10
CP1	Lack of intelligent devices for immediate defensive actions against terrorists	1.0
CP2	No sophisticated security measures and surveillance for CargoCap	0.50
CP3	Lack of stringent policy and technology for security and safety	0.50
CP4	Agencies in charge of developing and enforcing regulations remained "business-as-usual"	0.40
Ca	Terrorists' intrusion into CargoCap underground freight tunnel facilities near urban areas	0.40
Cb1	Placing of explosive devices at tunnel surfaces and in CargoCap freight systems	0.20
Cb2	Generated electromechanical and cyber-controller system failure	0.20
Cb3	Generated tubular rail security and sensor failure	0.20
Cb4	Generated CargoCap(s) damage and rupture	0.20
Cc	Explosion of CargoCap freight transport carrying HAZMAT: escape and emission of HAZMAT and rupture of CargoCap	0.75
Cd	HAZMAT emission due to CargoCap terrorism	0.85
Ce	Leaks of HAZMAT to the environment and nearby infrastructures	0.50
Cf1	Contaminated the adjacent environment with HAZMAT release after the attacks	0.95
Cf2	Disrupted other industries dependent on CargoCap freight transport systems	0.95
Cf3	Disrupted mobility of goods and HAZMAT products in urban areas	0.20
Cf4	Caused economic distress due to a need of transport system	0.10
Cf5	Caused public panic and damage to public confidence and morale	0.20

Table 7.26 Risk Rates Based on Engineering Judgment of the Event Tree Analysis for Underground Maglev Mass Transit System

Symbol	*Event Tree List of Events*	*Risk Rate*
MTa	Terrorists situated themselves near underground maglev mass transit system facilities	0.50
MT1	Lack of intelligent devices for immediate defensive actions against terrorists	1.0
MT2	No sophisticated security measures and surveillance for the underground maglev train systems	0.40
MT3	Lack of stringent policy and technology for security and safety	0.20
MT4	Agencies in charge of developing and enforcing regulations remained "business-as-usual"	0.10
Ma	Terrorists' intrusion into underground maglev mass transit facilities near urban areas	0.75
Mb1	Placing of explosive devices at tunnel surfaces and in maglev trains	0.20
Mb2	Generated electromechanical and cyber-controller system failure	0.20
Mb3	Generated maglev security and sensor failure	0.20
Mb4	Generated maglev trains damage and rupture	0.60
Mc	Explosion of maglev trains: escape and burst of hazardous debris from the collision and explosion of maglev	0.90
Md	Burst of missiles of sharp objects and collapse of tunnels, affecting ground surface	0.90
Me	HAZMAT emission due to maglev train accidents	0.20
Mf1	Mass casualties and injuries (hundreds to more than a thousand passengers may likely be involved)	0.80
Mf2	Contaminated the environment with HAZMAT release from the attack	0.10
Mf3	Disrupted other industries dependent on underground mass transit systems	0.75
Mf4	Disrupted mobility in urban areas or interstates dependent on maglev underground systems	0.85
Mf5	Caused economic distress due to a need of remediation and recovery	0.85
Mf6	Caused public panic and damage to public confidence and morale	0.95

Table 7.27 Risk Rates Based on Engineering Judgment of the Event Tree Analysis for Oil and Gas Pipelines

Symbol	*Event Tree List of Events*	*Risk Rate*
PP1	Terrorists situated themselves near oil and gas "gathering lines" (8 in. diameter pipelines)	0.25
PP2	Terrorists situated themselves near oil and gas "trunk lines" adjacent to shorelines	0.25
Pa	Lack of intelligent devices for immediate defensive actions against terrorists	1.0
Pb	No sophisticated security measures and surveillance for the oil and gas pipelines	0.20
Pc	Lack of stringent policy and technology for security and safety	0.40
Pd	Agencies in charge of developing and enforcing regulations remained "business-as-usual"	0.40
PPa	Terrorists' intrusion into the vicinity, then sabotage of oil and gas gathering lines	0.20
PPb	Terrorists sabotage oil and gas trunk lines near shorelines	0.20
PPa1	Generated explosions, pool fires, and jet flames and destroyed gathering lines	0.90
PPb1	Generated explosions, pools fires, and jet flames and destroyed a portion of trunk lines	0.90
PPa2	HAZMAT mixed in the atmosphere and contaminated the environment	0.80
PPa21	HAZMAT will not be treated immediately and affected the natural resources	0.20
PPa22	HAZMAT mixed with other pollutants present in the air and soil	0.50
PPa23	HAZMAT diluted in some areas by strong winds	1.0
PPb2	HAZMAT mixed in the atmosphere and severely contaminated the environment	0.80
PPb21	HAZMAT will not be treated immediately and severely affected the natural resources	0.80

Table 7.27 (continued) Risk Rates Based on Engineering Judgment of the Event Tree Analysis for Oil and Gas Pipelines

Symbol	*Event Tree List of Events*	*Risk Rate*
PPb22	HAZMAT mixed with other pollutants present in air, soil, and water (surface water and groundwater)	0.40
PPb23	HAZMAT diluted in some areas by strong winds	1.0
L1	Polluted the environment and caused destruction to natural resources	0.60
L2	Caused economic distress due to a need of environmental cleanup and recovery	0.50
L3	Disrupted the oil and gas pipelines company and refinery owners	0.50
L4	Caused damage to public confidence due to the fear of terrorist attacks	0.30
K1	Caused public health injury	0.60
K2	Caused economic distress due to a need of environmental cleanup and recovery	0.80
K3	Caused economic distress to owners due to a need of rebuilding the infrastructures	0.60
K4	Disrupted the oil and gas pipelines and refinery owners	0.60
K5	Caused damage to public confidence due to the fear of terrorist attacks	0.60

physical violence at first), then utilize stronger actions through threats and physical violence. This is a primary factor embedding the *military plan* which executes the power of the State to control and to overcome the enemy by isolating and occupying or dominating the enemy's territory. Therefore, *intuitive judgment in the military operations* in supporting homeland and critical infrastructure protection is vital for the success of effective employment of offensive and defensive strengths. Successful war against the enemy not only requires practical experience and fighting strength but also the ability to manufacture creative imagination and the capacity to have intuitive predictions. The risk assessment methodology incorporated with cumulative prospect theory (refer to Chapters 6 and 7) can be used to formulate intuitive estimates and to screen accurate prediction of outcomes quantitatively by analysts and decision makers in order to maintain mental power, clear vision, and provide clever recommendations to the State in terms of military operations.

Table 7.28 Risk Rates Based on Engineering Judgment of the Event Tree Analysis for the Risk of Secret Tunnels and WMD

Symbol	*Event Tree List of Events*	*Risk Rate*
ET2a-1	Terrorist leaders and supporters developed and constructed subterranean infrastructures for WMD fabrication, manpower distribution, and terror-military operations	0.90
ET2a-2	Constructed secret tunnels near metropolitan areas	0.35
ET2a-3	Built underground freight transportation system or maglev train for manpower mobilization, WMD materials transshipments, and support for terror-military operations, and used those infrastructures as a disguise system	0.35
ET2a-4	Built friendly relationships with other rebellious nations	0.40
ET2b-5	Constructed cross-border tunnels with other corrupt states for manpower and WMD materials transshipments	0.35
ET2a-6	Developed weapons and powerful WMD and terror-military operations for future conflicts Developed plans for intrusion or terror attacks defense and escape strategies	0.60
ET2a-8	Detonation of WMDs	0.50
ET2a-9	HAZMAT/radioactive material dispersion in the environment after WMD attacks	0.50
ET2a-10	HAZMAT/radioactive material mixed with other pollutants in the environment	0.80
ET2a-11	HAZMAT/radioactive material diluted in some areas	0.80
ET2a-12	Flush floods, if large water reservoirs and pipelines are destroyed by WMD detonation—flush floods gushing toward the downstream area	0.10
ET2a-13	Explosion of infrastructures: escape and burst of hazardous debris from the collapse of infrastructures	0.90
ET2a-14	Burst of missiles of sharp objects and other types of hazardous debris	0.90
ET2a-15	Catastrophic health effects	0.90

Table 7.28 (continued) Risk Rates Based on Engineering Judgment of the Event Tree Analysis for the Risk of Secret Tunnels and WMD

Symbol	*Event Tree List of Events*	*Risk Rate*
ET2a-16	Disrupted other industry infrastructures and caused economic collapse	0.90
ET2a-17	Contaminated the environment with hazardous debris	0.90
ET2a-18	No other immediate water, food, and medical supplies available after the WMD attacks	0.90
ET2a-19	No immediate supplies and medical health facilities because they are mostly destroyed	0.90
ET2a-20	Mass casualties and severe public injury: created damage to public psychology and morale	0.90
ET2a-21	Collapse of major infrastructures and a need of environmental cleanup and recovery	0.90

Table 7.29 Risk Assessment and Risk Acceptability Analysis Comparison for Pipelines, Tunnels, Rail, and Transit Systems and Clandestine Tunnels

Sl. No.	*Description*	*Risk Estimation*	*Risk Acceptability* $V(f) = \omega(p) \cdot \nu(x)$
1	Terrorist attack on tubular rail	1.3×10^{-3} (very high risk)	2.3×10^{-17} (unacceptable risk)
2	Terrorist attack on aqueduct (water pipeline)	5.0×10^{-4} (very high risk)	3.3×10^{-15} unacceptable risk)
3	Terrorist attack on CargoCap/underground freight transportation through pipelines	5.1×10^{-6} (very high risk)	2.3×10^{-17} (unacceptable risk)
4	Terrorist attack on magnetic levitation	2.3×10^{-6} (very high risk)	2.3×10^{-17} (unacceptable risk)
5	Terrorist attack on oil and gas pipelines	7.5×10^{-7} (very high risk)	2.2×10^{-15} (unacceptable risk)
6	Security risk of secret tunnels and WMD launch	9.2×10^{-4} (very high risk)	2.3×10^{-17} (unacceptable risk)

Table 7.30 Risk Acceptability Analysis Comparison of Alternatives for Pipelines, Tunnels, Rail, and Transit Systems

Sl. No.	*Description*	*Risk Reference*	*Proportionality by Degree of Voluntarism*	*Derating*	*Controllability*	*Risk Acceptability* $V(f)=\omega(p)\cdot\nu(x)$
1	Terrorist attack on tubular rail	9.8×10^{-8} Man-originated catastrophic involuntary	0.09	0.000065	4.1×10^{-5}	2.3×10^{-17}
2	Terrorist attack on aqueduct (water pipeline)	9.8×10^{-8} Man-originated catastrophic involuntary	0.09	0.000065	1.8×10^{-3}	3.3×10^{-15}
3	Terrorist attack on CargoCap/underground freight transportation through pipelines	9.8×10^{-8} Man-originated catastrophic involuntary	0.09	0.000065	4.1×10^{-5}	2.3×10^{-17}
4	Terrorist attack on magnetic levitation	9.8×10^{-8} Man-originated catastrophic involuntary	0.09	0.0081	4.1×10^{-5}	2.3×10^{-17}
5	Terrorist attack on oil and gas pipelines	9.8×10^{-8} Man-originated catastrophic involuntary	0.09	0.000065	3.9×10^{-3}	2.2×10^{-15}
6	Security risk of secret tunnels and WMD launch	9.8×10^{-8} Man-originated catastrophic involuntary	0.09	0.000065	4.1×10^{-5}	2.3×10^{-17}

Table 7.31 Risk Acceptability Analysis Comparison of Alternatives for Clandestine Tunnels

Alternatives	*Risk Estimation*	*Risk Acceptability* $V(f)=\omega(p)\cdot\nu(x)$
1. Employ the following: Existing or available preventive measures and enforced existing regulations		
a. Tubular rail	3.7×10^{-8} (high risk)	2.3×10^{-10} (unacceptable risk)
b. Aqueduct (water pipeline)	2.8×10^{-6} (high risk)	2.3×10^{-10} (unacceptable risk)
c. CargoCap/underground freight transportation through pipelines	2.3×10^{-8} (high risk)	2.3×10^{-11} (unacceptable risk)
d. Magnetic levitation	6.2×10^{-8} (high risk)	2.3×10^{-11} (unacceptable risk)
e. Oil and gas pipelines	6.9×10^{-6} (high risk)	1.6×10^{-11} (unacceptable risk)
f. Secret tunnels and WMD launch	1.8×10^{-7} (high risk)	
2. Implement the following: a. Enhanced intelligence enterprise plan (Figure 7.24) b. Military support to homeland and critical infrastructure protection (Figure 7.22) c. Practice intuitive judgments in policy making and decision making in terms of homeland and critical infrastructure protection d. Develop not only preventive measures but also "defensive" systems to deter, detect, and terminate/capture the enemy. Should also implement special technologies such as intelligent devices with designed safety—detection distances e. Develop safety easement or encroachment from a critical infrastructure in conjunction with preventive and defensive approaches	7.5×10^{-11} (low risk)	9.0×10^{-9} (acceptable risk)

One way for analyzing predictability is to ask questions: "If you were to consider 3 (three) options to dominate the enemy that you are about to stop them to develop powerful WMD, how many times would you be accurate in your judgment -which of the 3 will help you attain your mission?" Or "If you are deciding to develop technologies to detect, deactivate and deter land mines and you were to choose which one of the 5 (five) alternative operations is effective, financially feasible, and indestructible by the enemy, how frequent would you be correct in predicting of the 5 alternatives that will help you achieve your goal to defeat the enemy's weapons?" Quantitative risk acceptability analysis can *help experts to make adjustments* in their intuitive judgments and predictions, and they should avoid *overconfidence* in the decision-making process. Based on the literature research, the levels of overconfidence rise with ignorance. When ample valid information supports the outcomes that the experts generate, overconfidence does not exist. A deeply perceptive military decision for strategy and tactics can be achieved by

- Delineating salient objectives and goals that are able to precisely define the efforts that would lead to the desired end results beneath the potential events and outcomes
- Incorporating risk acceptability into military decision-making process as shown in Figure 7.22
- Planning the military operations with creative imagination and accurate predictions based on quantitative psychology of judgment (Figures 7.22 and 7.23)
- Providing illustrative and graphical demonstrations with clarity of well-synchronized maneuvers, showing details of the operations to aid decision-makers, military leaders, and warfighters
- Communicating the designed objectives, intentions, and plans unequivocally with dynamic demonstrations to guarantee a well-synchronized action
- Efficient, *timely*, and skillful command and control of such action

7.9.1 Command of the Armed Forces and the Chain of Command

Command directs the armed forces by a military leader. The period of no crises and conflicts is the time for dynamic exercises, training, mastery, and preparedness of the armed forces for future warfare and for ensuring refined action during actual combat. The leader should also be aware of not only the abilities but also the limitations of the armed forces. Recognizing the limitations of the armed forces is essential in considering and developing other means to counterbalance those constraints.

The *chain of command* constitutes vertical chains of joints from below the highest rank, through which authority and duty are disseminated. Through the chain of command, a military leader has the authority to demand a certain amount of initiative and duty with eagerness to establish his proposed military objectives.

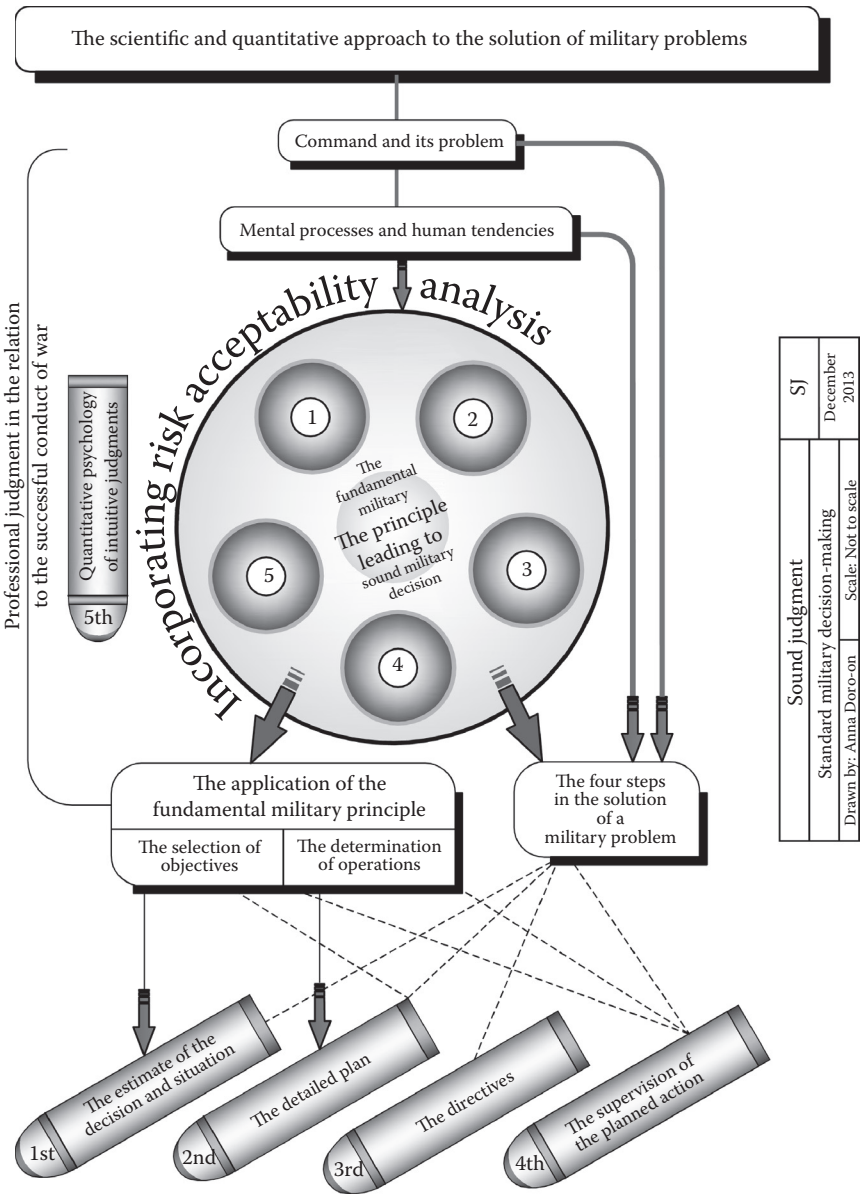


Figure 7.22 The standard military decision-making process. (From US Naval War College, *Sound Military Decision*, Naval Institute Press, Annapolis, MD, 1992.)

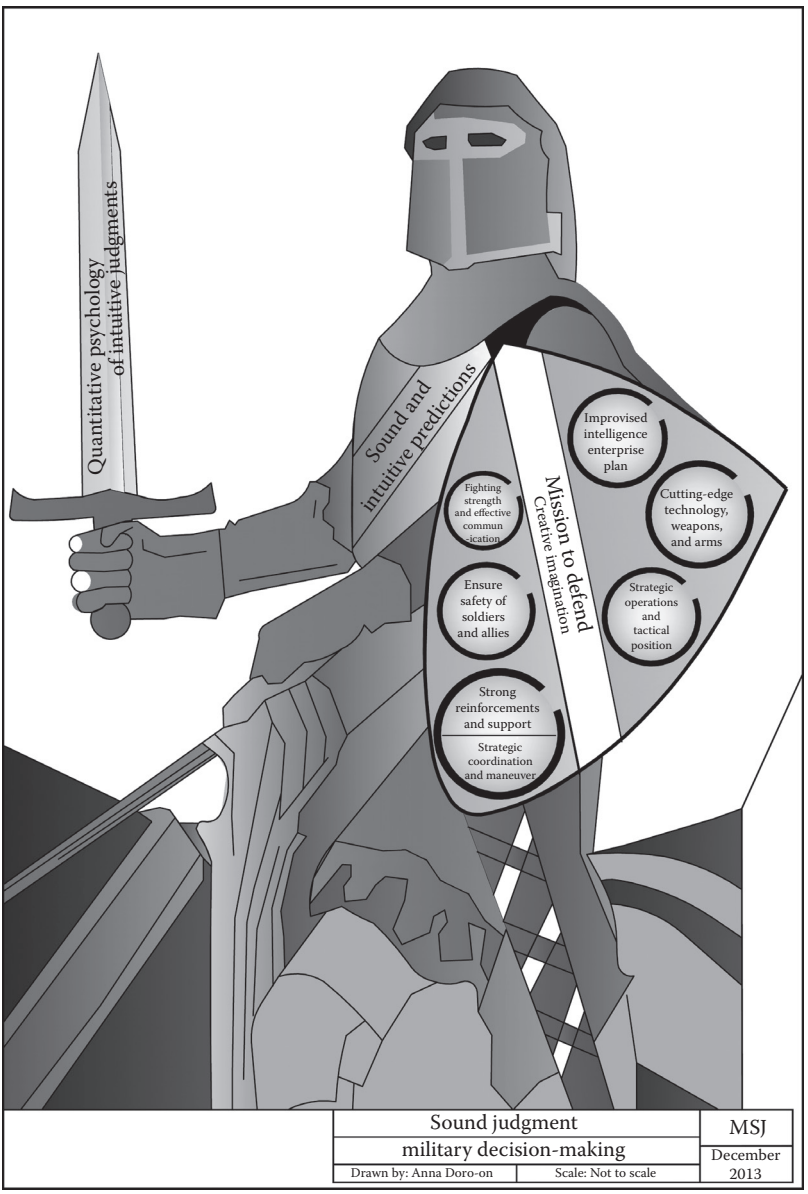


Figure 7.23 The modified military decision-making process.

He gives assignments to his direct subordinates and is responsible for executing his military plans. The completion of every duty he assigns shall engage the achievement of a given objective with mutual understanding throughout the chain of command.

7.9.2 Understanding Military Operations

A military operation is an endeavor or actions to fulfill a mission or goal having military aspects. It may usually comprise the overall defense campaign, definition of levels of execution in a war, military commands and control, identification of operations to attain military objective, reinforcement, and support, and standardized strategic procedure to achieve the mission and objective. A plan of action is critical to achieve military operations that support the main objective and it necessitates physical objects to achieve the overall objective. Systematic and salient plans of military operations include but are not limited to the following:

- The physical objectives involved
- The relative positions utilized
- The strong reinforcements and support—strategic coordination and maneuver
- The apportionment of fighting strength
- The preparation to be armed for freedom of action
- Efficient and effective action corresponding to correct physical objectives
- Projection of military action from advantageous relative positions
- Correct apportionment of fighting strength and effective communication
- Assurance of adequate freedom of action
- Assurance of safety of soldiers and allies

The effectiveness of a plan of military operations is based on sound and intuitive predictions in the military decision-making process (Figures 7.22 and 7.23) and the considerations rely on the following:

- Suitability of the planned actions, as determined by the factor of the appropriate effect desired
- Feasibility of the planned actions, by reason of relative fighting strength, as determined by the factors of the means available and opposed, influenced by the factors of the characteristics of the theater of operations
- Acceptability, as determined by the factor of the consequences as to costs and safety

Nevertheless, the risk assessment methodologies presented in Chapters 5 and 6 can provide a good perspective of the entire risks involved in the military operations to determine the suitability, feasibility, and acceptability of military operations in achieving the overall military objective. Military operation to support civilian law enforcement and to aid homeland protection is vital. The following

sections present the main components and regulations of military support for homeland and critical infrastructure security.

7.10 Requirement of Military Support for Critical Infrastructure and Homeland Security

For over a century the United States military has focused on expeditionary warfare overseas and, with the heightened concern about large-scale terrorism, has put in efforts to involve the DoD more closely with federal, state, and local agencies in their homeland security activities (Bowman 2003). In response to the increased focus on homeland security, on October 1, 2002, the DoD activated a new combatant command, the Northern Command (NORTHCOM) (Bowman 2003). The DoD makes a distinction between "homeland security" and "homeland defense" in defining its mission responsibilities as follows (Bowman 2003):

- Homeland security is a concerted "national" effort to prevent terrorist attacks within the United States, to reduce the vulnerability of the United States to terrorism, and to minimize the damage and assist in the recovery from terrorist attacks.
- Homeland defense is the "military" protection of US territory, domestic population, and critical defense infrastructure against external threats and aggression. It also includes routine, steady state activities designed to deter aggressors and to prepare US military forces for action if deterrence fails. In general, the DoD's contribution to homeland security can be divided into two general areas: deterrence and response (Bowman 2003).

According to the DoD (2003), there are three circumstances in which the DoD assets would be involved for homeland defense and civil support:

- In *extraordinary circumstances*, the DoD would conduct military missions such as combat air patrols or maritime defense operations. The DoD would take the lead in defending the people and the territory of the United States, supported by other agencies.
- In *emergency circumstances*, such as managing the consequences of a terrorist attack, natural disaster, or other catastrophe in support of civil authorities, the DoD could be asked to act quickly to provide capabilities that other agencies do not possess or that have been exhausted or overwhelmed.
- In *nonemergency circumstances of limited scope or planned duration*, the DoD would support civil authorities where other agencies have the lead—for example, providing security at a special event such as the 2002 Winter Olympics, or assisting other federal agencies to develop capabilities to detect chemical, biological, nuclear, and radiological threats.

The DoD is governed by myriad statutes and directives pertaining to the domestic use of the armed forces for any law enforcement action (Brake 2003). DoD Directive 3025.15, *Military Assistance to Civil Authorities*, provides basic policy guidelines for the Defense Department when supporting civilian law enforcement agencies (Brake 2003). When the DoD evaluates requests, it considers the following criteria before providing assistance (Brake 2003):

1. Legality—compliance with laws
2. Lethality—potential use of lethal force by or against DoD forces
3. Risk—safety of DoD forces
4. Cost—who pays and the impact on the DoD budget
5. Appropriateness—is the mission in the interest of DoD to conduct
6. Readiness—impacts of the requirement on the DoD's ability to perform its primary mission

7.10.1 Intelligence

According to the Office of the Director of National Intelligence (ODNI 2013), the following 17 members of the IC support the mission to protect and defend the United States:

1. *Office of the Director of National Intelligence*—Serves as the principal adviser to the President, National Security Council, and the Homeland Security Council (ODNI 2013).
2. *The Air Force Intelligence, Surveillance, and Reconnaissance (AFISR)*—Is the Air Force (AF) component that provides policy, oversight, and guidance to all AF intelligence organization (AFISR 2010).
3. *US Army Intelligence (G-2)*—Is responsible for policy formulation, planning, programming, budgeting, management staff supervision, evaluation, and oversight for intelligence activities for the Department of Army (USAI 2013).
4. *Central Intelligence Agency*—Is responsible for providing national security intelligence to senior US policy makers (CIA 2013).
5. *Coast Guard Intelligence*—Its responsibilities include protecting citizens from the sea, protecting America from threats delivered by the sea, and protecting the sea itself (USCG 2010).
6. *Defense Intelligence Agency (DIA)*—Is a DoD combat support agency (USCG 2010). DIA is the first in all-source defense intelligence to prevent strategic surprise and deliver a decision advantage to warfighters, defense planners, and policy makers (DIA 2013).
7. *Department of Energy's Office of Intelligence and Counterintelligence*—Is responsible for the intelligence and counterintelligence activities throughout the DOE complex, including more than 30 intelligence and counterintelligence offices nationwide (USCG 2010).

8. *Department of Homeland Security's Office of Intelligence*—Is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the United States (DHS 2013).
9. *Department of State's Bureau of Intelligence and Research*—Provides the Secretary of State with timely, objective analysis of global developments as well as real-time insights from all-source intelligence (DOS-BIR 2013).
10. *Department of the Treasury's Office of Intelligence Analysis*—Is responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information related to the operation and responsibilities of the Department of Treasury (US Department of the Treasury 2013).
11. *Drug Enforcement Administration*—Is responsible for enforcing the controlled substance laws and regulations of the United States (DEA 2013).
12. *Federal Bureau of Investigation*—Is responsible for understanding threats to our national security and penetrating national and transnational networks that have a desire and capability to harm the United States (FBI 2013).
13. *Marine Corps Intelligence*—Is comprised of all intelligence professionals in the Marine Corps responsible for policy, plans, programming, budgets, and staff supervision of intelligence and supporting activities within the US Marine Corps (USMC 2013).
14. *National Geospatial-Intelligence Agency*—Provides timely, relevant, and accurate geospatial intelligence in support of national security objectives (NGIA 2013).
15. *National Reconnaissance Office*—Designs, builds, and operates the nation's reconnaissance satellites (NRO 2013).
16. *National Security Agency/Central Security Service*—Is the nation's cryptologic organization that coordinates, directs, and performs highly specialized activities to protect US information systems and to produce foreign signals intelligence information (NSA/CSS 2013).
17. *Navy Intelligence*—Is the leading provider of maritime intelligence to the US Navy and warfighting forces, as well national decision makers and other consumers in the IC (ONI 2013).

7.10.2 Northern Command

The US Northern Command (USNORTHCOM) is a regional combatant command with an area of responsibility (AOR) that includes the continental United States, Alaska, Canada, Mexico, and surrounding waters out to approximately 500 nautical miles, including the Gulf of Mexico and the Straits of Florida (Joint Chiefs of Staff 2005; Knight 2008; USNORTHCOM 2013a). USNORTHCOM AOR also includes portions of the Caribbean region to include The Bahamas, Puerto Rico, and the US Virgin Islands (USNORTHCOM 2013a). Army, Air Force, and Marine Corps components are assigned to USNORTHCOM, while

Navy Fleet Forces Command is a supporting component (Knight 2008). These service component commands provide an administrative framework to command service forces gained from US Joint Forces Command (JFCOM) for specific contingency component (Knight 2008). USNORTHCOM (2013a) has subordinate commands:

1. *Joint Force Headquarters National Capital Region* is responsible for land-based homeland defense, defense support of civil authorities, and incident management in the National Capital Region.
2. *Joint Task Force Civil Support* plans and integrates DoD support to the designated Primary Agency for domestic chemical, biological, radiological, nuclear, and explosives (CBRNE) consequence management operation.
3. *Joint Task Force North* is to support our nation's federal law enforcement agencies in the interdiction of suspected transnational threats within and along the approaches to the continent of United States.
4. *Army North* assigns Defense Coordinating Officers to all 10 FEMA regional offices to streamline DoD coordination (Knight 2008).
5. *Air Force North* is responsible for developing and unifying the military response capability for CBRNE incidents.
6. *US Fleet Forces Command* is to provide maritime forces.
7. *US Marine Forces Northern Command* is responsible for force-protection of Marine installations and for assisting NORTHCOM civil support planning; the command has 32 Marine Emergency Preparedness Liaison Officers focused on specific Federal Emergency Management Agency (FEMA) regions (Knight 2008).
8. *US Special Operations Command*, North (Provisional Command), is a new command approved in December 2012 as a subordinate unified command under USNORTHCOM and is scheduled to enhance control of special operations forces throughout the USNORTHCOM AOR in 2014 (USNORTHCOM 2013a).

7.10.3 Department of Defense: Chemical, Biological, Radiological, and Nuclear Incident Response

According to the Joint Chiefs of Staff Joint Publication 3-41 (2012), due to the potential catastrophic nature of a CBRN incident, a DoD Joint Force may be called upon to assist with a civilian CBRN incident prior to civilian resources being overwhelmed or depleted. The Secretary of Defense designated supported of the JFC is ultimately responsible for the DoD CBRN response and its role in providing resources to mitigate the consequences of the CBRN incident (Joint Chiefs of Staff 2012). Many DoD strategies, activities, and programs support preparation for a CBRN response; examples include unit training, and local, regional, national, and

international-level environments (Joint Chiefs of Staff 2012). The DoD CBRN capabilities are divided into seven elements:

1. CBRN CM Command and Control Element
2. CBRN Reconnaissance and Surveillance Element
3. CBRN CM Decontamination Element
4. CBRN CM Medical Element
5. CBRN CM Force Protection Element
6. Search and Rescue Element
7. General Support Element

The Joint Chiefs of Staff Joint Publication 3-40, 2009, stated that the National Strategy to Combating Weapons of Mass Destruction (NS-CWMD) provides additional guidance concerning CWM: NP, CP, and WMD consequence management (CM), as highlighted in the National Security Strategy (NSS), and introduces the construct of the three pillars which provides a common framework for the interagency conduct of CWMD activities. The NSS is identified as an essential task to "prevent our enemies from threatening us, our allies, and our friends with WMD" for ensuring national security (Joint Chiefs of Staff 2009).

Combating WMD (CWMD) requires a long-term, strategic approach that places heavy emphasis on interagency support and international coordination and cooperation to create an environment that is inhospitable to the acquisition, development, proliferation, and use of WMD, denying adversaries safe haven, and disrupting WMD-enabling networks (Joint Chiefs of Staff 2009). The Joint Chiefs of Staff (2009) stated that the essential efforts of CWMD are as follows:

1. *CWMD Operational Environment* is the global nature of the operational environment.
2. *Shaping Activities* are performed to dissuade or deter potential adversaries and to assure or solidify relationships with friends and allies.
3. *CWMD and Major Contingencies*, CWMD should be integrated throughout major contingency planning and execution to ensure successful prosecution.
4. *Nonproliferation* comprises those actions taken to prevent the proliferation of WMD.
5. *Counterproliferation* comprises those actions taken to defeat the threat and/or use of WMD.
6. *WMD Consequence Management* consists of those actions authorized by the President or Secretary of Defense to mitigate the effects of a WMD attack or event and provide temporary essential operations and services at home and abroad.

7.10.3.1 US Army Chemical Material Agency

The US Army Chemical Material Agency (CMA) was one of the organizations derived from the former US Army Soldier and Biological Chemical Command (SBCCOM) in October 2003. SBCCOM was remodeled into five organizations: CMA; US Army Research, Development, and Engineering Command (RDECOM); Guardian Brigade; US Army Nuclear, Biological, and Chemical Defense (PM NBC); and Soldiers System Center (SSC) to have a better focus and to enhance defense capabilities. Hence, CMA safely stores and destroys the United States' aging chemical weapons and effectively recovers chemical warfare material and treats it and enhances national security (CMA 2012). The activity also partners with FEMA to ensure the emergency preparedness of the communities surrounding the depots where stockpiled chemical weapons are stored (CMA 2012).

7.10.3.2 US Army Research, Development, and Engineering Command

The Research, Development, and Engineering Command (RDECOM) ensures the dominance of Army capabilities by creating, integrating, and delivering technology-enabled solutions to warfighters and develops technologies in its eight major laboratories and research, development, and engineering centers (RDECOM 2013a). Edgewood Chemical Biological Center (ECBC) supports RDECOM in its chemical, biological, radiological, nuclear, and explosives defense needs (RDECOM 2013b). The ECBC has a long-standing history of developing technologies in the areas of chemical and biological detection, protection, and decontamination (RDECOM 2013b).

7.10.3.3 US Army—20th Support Command Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Analytical Remediation Activity

The 20th Support Command Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Analytical Remediation Activity (CARA-West; formerly known as the *US Army Technical Escort Unit*), which took over the Guardian Brigade, has multiple skills including all chemical and biological support; however, a forensic laboratory has been set up as part of CARA (DOA 2009).

7.10.3.4 US Army—20th Support Command Chemical, Biological, Radiological, Nuclear, and Explosives

The 20th Support Command Chemical, Biological, Radiological, Nuclear, and Explosives (20th SUCOM CBRNE) provides highly trained, properly equipped,

disciplined, and well-led forces to counter the entire range of CBRNE ordnance hazards for the United States (DOA 2013). It gives the Army and the nation a scalable response capability with the flexibility to operate in a variety of environments, from urban areas to austere sites across the spectrum of military operations (DOA 2013). On order, the 20th SUCOM CBRNE deploys, provides command and control for the Army and/or Joint Task Force specialized CBRNE forces to execute specialized CBRNE operations, and provides technical capabilities and CBRNE subject matter expertise to Joint Task Force and Army commanders to achieve national combating WMD objectives (20th SUCOM 2011).

7.10.3.5 Joint Program Executive Office for Chemical and Biological Defense

The Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) supports the DoD, which works side by side with the Department of Homeland Security and other agencies in the ongoing effort to guard against CBRN threat. The JPEO-CBD develops and tests, acquires, and delivers the world's most effective automated Biological Detection Systems, Medical Diagnostics and Countermeasures (JPEO-CBD 2010).

7.10.3.6 National Guard Weapons of Mass Destruction: Civil Support Teams

The National Guard (NG) leverages its warfighting capability to support the civil authorities by providing a disciplined, well-trained, and well-equipped organization to supplement local, state, and Federal efforts to manage potential catastrophic events, or provide special technical support to augment specific needs of the Incidental Commander (IC) (NGB 2011). Weapons of Mass Destruction—Civil Support Teams (WMD-CSTs) are designed and trained to provide initial assessment of incidents and advise and assist the IC, State Emergency Management, the State's Joint Forces Headquarters (JFHQ-State), the Adjutant General (AG) or Commanding General (CG), the Governor, and other key officials, including synchronized, integrated, and seamless WMD-CST employment, across the nation on short notice to assist local and state governments in protecting public health and safety, restoring essential government services, and providing emergency relief to governments, businesses, and individuals affected by the consequences of catastrophic events as outlined in 10 USC §12310 (NGB 2011). The WMD-CSTs are NG units designed to provide a specialized capability to respond to a chemical, biological, radiological, or nuclear (CBRN) incident primarily in a Title 32 operational status within the United States, the District of Columbia, its territories and possessions, as established by 10 USC §12310 (NGB 2011).

7.10.3.7 US Army Special Operations Command

US Army Special Operations Command is the largest of the service components that make up the US Special Operations Command and provides about 70% of the special operations personnel in Central Command's theater (USASOC 2013a). Its duties are to organize, train, educate, man, equip, fund, administer, mobilize, deploy, and sustain Army special operations forces to successfully conduct worldwide special operations, across the range of military operations, in support of regional combatant commanders, American ambassadors, and other agencies as directed (USASOC 2013a). In addition to reporting to the Department of the Army, USASOC also functions as the Army component of the US Special Operations Command (USSOCOM), located at MacDill Air Force Base, Florida. USSOCOM is the congressionally mandated, unified combatant command responsible for all DoD special operations forces within the Army, Navy, Air Force, and Marine Corps (USASOC 2013b). The command also provides oversight of Army National Guard special operations forces' readiness, organization, training, and employment in coordination with the National Guard Bureau and state adjutants general (USASOC 2013b). USASOC's major subordinate commands include the US Army Special Forces Command (Airborne), the US Army John F. Kennedy Special Warfare Center and School, and the US Army Special Operations Aviation Command, all located at Fort Bragg, North Carolina. Its major subordinate units include the 75th Ranger Regiment at Fort Benning, Georgia; the 160th Special Operations Aviation Regiment (Airborne) at Fort Campbell, Kentucky; the Military Information Support Operations Command (Airborne) (Provisional); the 95th Civil Affairs Brigade (Airborne); and the Sustainment Brigade (Special Operations) (Airborne), all at Fort Bragg, North Carolina (USASOC 2013b).

7.10.4 Posse Comitatus Act: USC Title 18, §1385

The *Posse Comitatus Act* (PCA) prohibits the use of the military in activities such as arrest, seizure of evidence, search of person, search of building, investigation of a crime, interviewing witnesses, pursuit of an escaped prisoner, search of an area for a suspect, and other similar activities (DOJ 2000; Brake 2003). The PCA does not apply to the US Coast Guard in peacetime or to the National Guard in Title 32 or State Active Duty status (USNORTHCOM 2013b). The substantive prohibitions of the PCA were extended to all the services with the enactment of Title 10 USC, §375. As required by Title 10 USC, §375, the secretary of defense issued DoD Directive 5525.5, which precludes members of the Army, Navy, Air Force, or Marine Corps from direct participation in a search, seizure, arrest, or other similar activity unless participation in such an activity by such a member is otherwise authorized by law (USNORTHCOM 2013b). The United States Congress has enacted a number of exceptions to the PCA that allow the military, in certain

situations, to assist civilian law enforcement agencies in enforcing the laws of the United States. The most common example is counterdrug assistance (Title 10 USC, §371–381) (USNORTHCOM 2013b). The PCA aside, it appears that the president may not use the military to (Doyle 2001)

- Seize an industry critical to national security even in a national emergency when Congress has declined to empower him to do so, *Youngstown Co. v. Sawyer*, 343 US 579 (1952)
- Subject civilians to military tribunals for criminal prosecution while civilian courts remain available, *Reid v. Covert*, 354 USC 1 (1957); *Exparte Milligan*, 71 US (4 Wall.) 2 (1866)
- Compel state officials to execute federal authority, *Printz v. United States*, 521 US 898 (1997)
- Restrictions on use of the National Guard (until federalized) are matter of state law which varies from jurisdiction to jurisdiction

The House of Representatives (H.R.) 1986 would amend title 10 to allow the Secretary of Defense to provide military personnel to assist the Department of Homeland Security when necessary to respond to *a threat to national security posed by the entry into the United States of terrorists, drug traffickers, or illegal aliens* (Elsea 2005). Military members would first have to undergo training in issues related to law enforcement in border areas and would have to be accompanied by civilian law enforcement officers. H.R. 1986 passed the House as section 1035 of the National Defense Authorization Act for FY2006 (H.R. 1815), but without a limitation that would have ended the authority after September 30, 2007 (Elsea 2005). Senate Bill *S. 1042* and *S. 1043*, the Senate Defense authorization bills, would add a new section 383 to Title 10, which would authorize the Secretary of Defense to use unmanned aerial vehicles and DoD personnel to conduct aerial reconnaissance within the US NORTHCOM's AOR, in order to monitor air and sea traffic along the border and coastline, and to communicate resulting information to the appropriate federal, state, and local law enforcement officials. The activity would be funded from counterdrug appropriations (Elsea 2005). The prohibitions against military personnel participating in searches, seizures, or arrests would apply (Elsea 2005).

7.10.5 Insurrection Act: USC Title 10, §331–335, Chapter 15

The Insurrection Act allows the president to use US military personnel at the request of a state legislature or governor to suppress insurrections (USNORTHCOM 2013b). It also allows the president to use federal troops to enforce federal laws when rebellion against the authority of the United States makes it impracticable to enforce the laws of the United States (USNORTHCOM 2013b). The four sections of the act are as follows (Brinkerhoff 2009):

- Title 10, §331 was enacted in 1792 in response to challenges to the taxing power of the federal government. It allows the President, at the request of a governor or state legislature, to put down an insurrection by calling into federal service sufficient militia to "*suppress the insurrection*."
- Title 10, §332 was enacted in 1861 at the outset of the Civil War. It allows the President to use the armed forces to enforce the laws or suppress a rebellion whenever, in his opinion, unlawful obstructions, combinations, or assemblages or rebellion against the authority of the United States make it impractical to enforce the laws using the course of judicial proceedings.
- Title 10, §333 was enacted in 1869 during the Reconstruction Era. It allows the President to use the armed forces or militia to respond to insurrection, domestic violence, unlawful combination, or conspiracies that prevent a state government from enforcing the laws.
- Title 10, §334 was enacted in 1861. It prescribes that the President shall issue a proclamation calling on insurgents to disperse before using the militia or armed forces to enforce the law.

7.10.6 Military Support to Civilian Authorities: USC Title 10, §371–382, Chapter 18

The Secretary of Defense has explicit statutory authority to permit assistance to state and local enforcement (on a reimbursable basis, 10 USC §377), without adversely affecting military preparedness (10 USC §376), and without using personnel to conduct searches or arrests (10 USC §375) in the form of (Doyle 2001)

- Sharing intelligence gathered in military operations, 10 USC §371
- Supplying military equipment and facilities, 10 USC §372
- Providing training and advising on the use and maintenance of equipment, 10 USC §373
- Maintaining and operating equipment, 10 USC §374

7.10.7 Military Support: Maintenance of Other Troops: USC Title 32, §109, Chapter 1

The USC Title 32, §109, Chapter 1, stated the following (United States Code 2012a):

a. In times of peace, a State, the Commonwealth of Puerto Rico, the District of Columbia, Guam, or the Virgin Islands may maintain no troops other than those of its NG and defense forces authorized by subsection (c).
b. Nothing in this title limits the right of a State, the Commonwealth of Puerto Rico, the District of Columbia, Guam, or the Virgin Islands to use

its NG or its defense forces authorized by subsection (c) within its borders in times of peace, or prevent it from organizing and maintaining police or constabulary.

c. In addition to its NG, if any, a State, the Commonwealth of Puerto Rico, the District of Columbia, Guam, or the Virgin Islands may, as provided by its laws, organize and maintain defense forces. A defense force established under this section may be used within the jurisdiction concerned, as its chief executive considers necessary, but it may not be called, ordered, or drafted into the armed forces.
d. A member of a defense force established under subsection (c) is not, because of that membership, exempt from service in the armed forces; nor is he entitled to pay, allowances, subsistence, transportation, or medical care or treatment from funds of the United States.
e. A person may not become a member of a defense force established under subsection (c) if he is a member of a reserve component of the armed forces.

7.10.8 National Guard for Homeland Defense Duty: USC Title 32, §904, Chapter 9

The USC Title 32, §904, stated the following (United States Code 2012b):

a. *Full-Time NG Duty*—all duty performed under this chapter shall be considered to be full-time NG duty under section 502 (f) of this title.
b. *Duration*—The period for which a member of the NG performs duty under this chapter shall be limited to 180 days. The Governor of the State may, with the concurrence of the Secretary of Defense, extend the period one time for an additional 90 days to meet extraordinary circumstances.
c. *Relationship to Required Training*—A member of the NG performing duty under this chapter shall, in addition to performing such duty, participates in the training required under section 502 (a) of this title.
d. *Readiness*—To ensure that the use of units and personnel of the NG of a State for homeland defense activities does not degrade the training and readiness of such units and personnel, the following requirements shall apply in determining the homeland defense activities that units and personnel of the NG of a State may perform.
e. The performance of the activities is not to affect adversely the quality of that training or otherwise interfere with the ability of a member or unit of the NG to perform the military functions of the member or unit.
f. The performance of the activities is not to degrade the military skills of the members of the NG performing those activities.

7.10.9 Response to Threats of Terrorist Use of Weapons of Mass Destruction: USC Title 50, §2311, Chapter 40

According to the USC Title 50, §2311 (2012c), based on the DoD reference (2012), responses to threats of terrorists' use of WMD

a. Enhance response capability—in light of the potential for terrorists' use of WMD against the United States, the president shall take immediate action
   1. To enhance the capability of the Federal Government to prevent and respond to terrorist incidents involving WMD
   2. To provide enhanced support to improve the capabilities of State and local emergency response agencies to prevent and respond to such incidents at both the national and the local levels
b. Report required, not later than January 31, 1997—the President shall transmit to Congress a report containing
   1. An assessment of the capabilities of the Federal Government to prevent response to terrorist incidents involving WMD and to support State and local prevention and response efforts
   2. Requirements for improvements in those capabilities
   3. The measures that should be taken to achieve such improvements, including additional resources and legislative authorities that would be required

7.10.10 Presidential Policy Directive 8

The Presidential Directive 8 is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the nation, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters (USWH 2011). Our national preparedness is the shared responsibility of all levels of government, the private and nonprofit sectors, and individual citizens (USWH 2011). The Secretary of Homeland Security shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the nation's critical infrastructure. In carrying out the responsibilities assigned in the Homeland Security Act of 2002, as amended, the Secretary of Homeland Security evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security and resilience functions that are necessary for effective public–private engagement with all critical infrastructure sectors; develops a national plan and metrics, in coordination with Sector-Specific Agencies (SSAs)

and other critical infrastructure partners; integrates and coordinates Federal cross-sector security and resilience activities; identifies and analyzes key interdependencies among critical infrastructure sectors; and reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure (USWH 2011).

According to FEMA (FEMA 2013a), there is one framework for each of the five preparedness mission areas addressed in PPD-8, as follows:

- Prevention—The Prevention mission area comprises *the capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism*. It is focused on ensuring that we are optimally prepared to prevent an imminent terrorist attack within the United States (FEMA 2013b).
- Protection—The Protection framework houses the capabilities necessary to secure the homeland against acts of terrorism and man-made or natural disasters (FEMA 2013b).
- Mitigation—Mitigation comprises the capabilities necessary to reduce the loss of life and property by lessening the impact of disasters (FEMA 2013b).
- Response—Response comprises the capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred (FEMA 2013b).
- Recovery—Recovery comprises the core capabilities necessary to assist communities affected by an incident to recover effectively (FEMA 2013b).

A secure and resilient nation has the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk (FEMA 2013c). These risks include events such as natural disasters, disease pandemics, chemical spills, and other man-made hazards, terrorist attacks, and cyber attacks (FEMA 2013c) (see Chapter 8). The National Preparedness Goal identified 31 core capabilities—these are the distinct critical elements needed to achieve the goal (FEMA 2013d): (1) planning; (2) public information and warning; (3) operational coordination; (4) forensics and attribution; (5) intelligence and information sharing; (6) interdiction and disruption; (7) screening, search, and detection; (8) access control and identity verification; (9) cyber security; (10) physical protective measures; (11) risk management for protection programs and activities; (12) supply chain integrity and security; (13) community resilience; (14) long-term vulnerability reduction; (15) risk and disaster resilience assessment; (16) threats and hazard identification; (17) critical transportation; (18) environmental response/health and safety; (19) fatality management services; (20) infrastructure systems; (21) mass care services; (22) mass search and rescue operations; (23) on-scene security and protection; (24) operational communication; (25) public and private services and resources; (26) public health and medical services; (27) situational assessment; (28) economic recovery; (29) health and social services; (30) housing; and (31) natural and cultural resources.

7.10.11 Manual for Civil Emergencies: DoD3025.1M

The Manual for Civil Emergencies (DoD3025.1M) provides guidance for the preparation, coordination, and execution of military support to civil authorities during civil emergencies within the United States, its territories, and possessions (DoD 1994). All those activities and measures are designed or undertaken (DoD 1994)

a. To minimize the effects upon the civilian population, or those that would be caused by an attack upon the United States
b. To deal with the immediate emergency conditions that would be created by any such attack
c. To effectuate emergency repairs to, or the emergency restoration of, vital utilities and facilities destroyed or damaged by any such attack

In terms of military support to civil authorities, these activities and measures are taken by the DoD components to foster mutual assistance and support between the DoD and any civil government agency in planning or preparedness for, or in the application of resources for response to, the consequences of civil emergencies or attacks, including security emergencies (DoD Directive 3025.1, reference (c)) (DoD 1994).

7.10.12 Military Support to Civilian Authorities: DoDD 3025.1

The DoD Directive 3025.1 is to consolidate all policy and responsibilities previously known as Military Assistance to Civil Authorities (MACA), applicable to disaster-related civil emergencies within the United States, its territories, and possessions under reference (a) (DoD Directive 3025.1), with those related to attacks on the United States, which previously were known as Military Support to Civil Defense (MSCD) under reference (b) (DoD Directive 3025.10) (DoD 1993). It is to provide for continuation of the DoD Regional Military Emergency Coordinator (RMEC) teams, previously developed under reference (c) (DoD Directive 5030.45), to facilitate peacetime planning for MSCA, and to provide trained teams of DoD liaison personnel to represent essential DoD components, as appropriate, for response to any national security emergency (DoD 1993). It is to constitute a single system for MSCA which shall plan for, and respond to, requests from civil government agencies for military support in dealing with the actual or anticipated consequences of civil emergencies requiring Federal response, or attacks, including national security emergencies as defined in reference (d) (Executive Order 12656) (DoD 1993). It is to state the policy and responsibilities by which the DoD responds to major disasters or emergencies in accordance with the Stafford Act and Federal or State civil defense programs, in cooperation with FEMA, under the authority of the Federal Civil Defense Act of 1950. It is to designate the Secretary of the Army (SOA) as the DoD executive agent for MSCA and to authorize the publication of DoD 3025.1M.

7.10.13 Military Assistance to Civilian Authorities: DoDD 3025.15

According to the DoD Directive 3025.15 (DoD 1997), the DoD shall cooperate with and provide military assistance to civil authorities as directed by and consistent with applicable law, Presidential directives, executive orders, and the Directive. All requests by civil authorities for DoD military assistance shall be evaluated by DoD approval authorities against the following criteria: legality; lethality; risk; cost; appropriateness; and readiness. The SOA is the approving authority for emergency support in response to natural or man-made disasters, as specified by the Directive (DoD 1997). The Secretary of Defense retains approving authority for support to civil authorities involving the use of forces assigned by the Commander in Chief, DoD support to civil disturbances, DoD responses to acts of terrorism, and DoD support that will result in a planned event with the potential for confrontation with specifically identified individuals and/or groups, or will result in the use of lethal force (DoD 1997). Nothing in this Directive prevents a commander from exercising his/her immediate emergency response authority as outlined in DoD Directive 3025.1 (DoD 1997). The Chairman of the Joint Chiefs of Staff (JCS) shall evaluate each request to use Combatant Command forces or equipment to determine if there is a significant issue requiring Secretary of Defense approval (DoD 1997). DoDD 3025.15 does not address non-Federalized NG assets in support of local and/or State civil agencies approved by the Governor (DoD 1997). Therefore, the Director of Military Support shall keep the Chairman of the JCS and the Secretary of Defense informed of such support (DoD 1997).

7.11 Implication

The risk assessment and risk acceptability analysis based on quantitative psychology, which is the cumulative prospect theory, is critical in the processes of defining risks and security or defense options for homeland and critical infrastructure. Normally, the decision maker tends to disregard very small probabilities based on standard risk assessments that can gravely compromise national security and public safety. In cumulative prospect theory, it is critical to inflate small extreme events (*e.g., terrorist attacks on the rail transportation system carrying bomb materials and the security risk of the development of WMD in clandestine tunnels*) which happen with small probability, rather than to deflate or disregard all small probability events. Moreover, "defensive systems" to detect, deter, and terminate or disable the enemy should also be incorporated, and not just preventive or protective measures taken for homeland and critical infrastructure security. Implementing correct salient homeland and critical infrastructure protection should objectively consider the following (Figure 7.24):

- Improvised intelligence analysis
- Enhanced intelligence enterprise plan

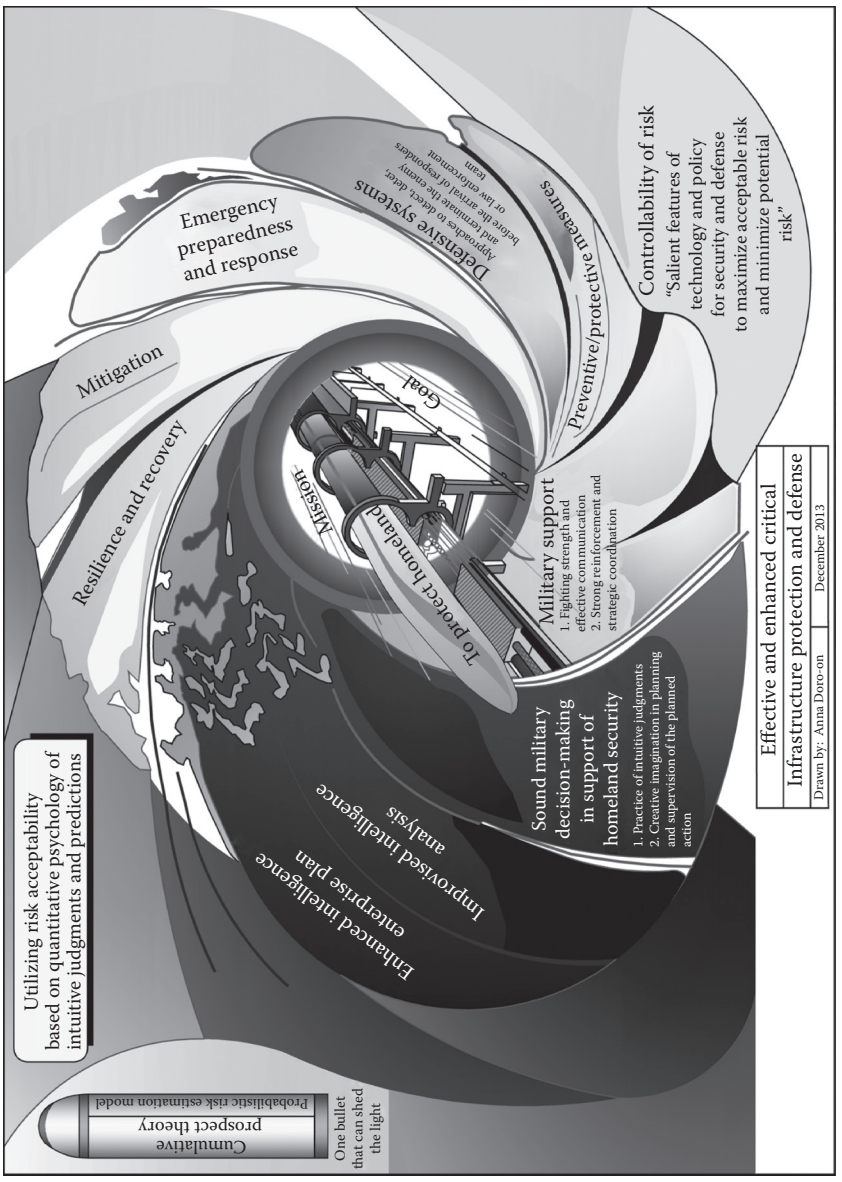


Figure 7.24 The modified military decision-making process effective and enhanced critical infrastructure protection.

- Intuitive and sound military decision making in support to homeland security
- Military support
- Preventive/protective measures
- Defensive systems and intelligent technologies to detect the enemy's actions and their weapons
- Emergency, preparedness, and response
- Mitigation
- Resilience and recovery

Chapter 8 introduces preparedness, preventive, and defensive measures.

References

Air Force Intelligence, Surveillance and Reconnaissance Agency. 2010. AFISR Agency fact sheet. http://www.af.mil/information/factsheets/factsheet.asp?id=9438 (accessed April 9, 2013).

BBC News. 2013. North Korea carries out biggest nuclear test. http://www.bbc.com/news/world-asia-21421841 (accessed February 13, 2013).

Bowman, S. 2003. Homeland security: The Department of Defense's role, report for Congress, order code RL31615. http://www.fas.org/man/crs/RL31615.pdf (accessed February 21, 2013).

Brake, J. 2003. Terrorism and the military's role in domestic crisis management: Background and issues for Congress. http://www.au.af.mil/au/awc/awcgate/crs/rl30938.pdf (accessed April 9, 2013).

Brinkerhoff, J. 2009. The role of federal military forces in domestic law enforcement title. http://usacac.army.mil/cac2/call/docs/10-16/ch_11.asp (accessed April 4, 2013).

Doro-on, A. 2011. *Risk Assessment for Water Infrastructure Safety and Security*. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Doyle, C. 2001. Terrorism: Some legal restrictions on military assistance to domestic authorities following a terrorist attack. CRC Report Congress, Order Code RS 1012. http://www.hsdl.org/?view&did=712192 (accessed January 5, 2013).

Drug Enforcement Administration. 2013. DEA fact sheet. http://www.justice.gov/dea/docs/factsheet.pdf (accessed April 9, 2013).

Elsea, J. 2005. The Posse Comitatus Act and related matters: A sketch. http://www.history.navy.mil/library/online/posse%20comit.htm (accessed April 12, 2013).

Ericson, C. 2005. *Hazard Analysis Techniques for System Safety*. Hoboken, NJ: John Wiley & Sons, Inc.

Federal Bureau of Investigation. 2013. National Security Branch. http://www.fbi.gov/about-us/nsb (accessed April 9, 2013).

Freedberg, S. 2013. North Korean nuclear threat drives army wargame; service shifts to rebuild WMD skills. http://defense.aol.com/2013/02/14/north-korean-nuclear-threat-drives-army-counter-wmd-wargame/ (accessed February 16, 2013).

Johnston, R. 2005. Analytic culture in the US Intelligence Community. Center for the Study of Intelligence, Central Intelligence Agency. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/full_title_page.htm (accessed October 16, 2012).

Joint Program Executive Office for Chemical and Biological Defense. 2010. Mission and vision. http://www.jpeocbd.osd.mil/packs/Default.aspx?pg=10 (accessed April 13, 2013).

Knight, W. 2008. Homeland security: Roles and missions for United States Northern Command. CRS Report for Congress, Order Code RL34342. http://www.fas.org/sgp/crs/homesec/RL34342.pdf (accessed April 10, 2013).

Lee, R. 2008. Why nuclear smuggling matters. http://www.fpri.org/orbis/5203/lee.nuclearsmuggling.pdf (accessed January 25, 2013).

National Geospatial-Intelligence Agency. 2013. NGIA mission. https://www1.nga.mil/Pages/default.aspx (accessed April 9, 2013).

National Guard Bureau. 2011. Weapons of Mass Destruction Civil Support Team Management. National Guard Regulation 500-3/Air, National Guard Instruction 10-2503. http://www.ngbpdc.ngb.army.mil/pubs/10/angi10_2503.pdf (accessed April 13, 2013).

National Reconnaissance Office. 2013. About the NRO, develop, acquire, launch, operate. http://www.nro.gov/about/index.html (accessed April 9, 2013).

National Security Agency/Central Security Service. 2013. Mission. http://www.nsa.gov/ (accessed April 9, 2013).

Nikitin, M. 2013. North Korea's nuclear weapons: Technical issues, congressional research service. http://www.fas.org/sgp/crs/nuke/RL34256.pdf (accessed February 18, 2013).

O'Connor, T. 2008. Border Security. http://drtomoconnor.com/3430/3430lect05.htm (accessed February 3, 2008).

Office of the Director of National Intelligence. 2013. Members of the intelligence community. http://www.dni.gov/index.php/intelligence-community/members-of-the-ic (accessed April 9, 2013).

Squassoni, S. 2006. Weapons of mass destruction: Trade between North Korea and Pakistan, CRC report for Congress. http://www.fas.org/sgp/crs/nuke/RL31900.pdf (accessed February 2, 2013).

United States Code. 2012a. USC Title 32: National Guard. http://uscode.house.gov/download/pls/Title_32.txt (accessed April 2, 2013).

United States Code. 2012b. 32 USC 9-Homeland defense activities. http://www.gpo.gov/fdsys/search/pagedetails.action?collectionCode=USCODE&searchPath=Title+32%2FCHAPTER+9&granuleId=USCODE-2011-title32-chap9&packageId=USCODE-2011-title32&oldPath=Title+32%2FChapter+9%2F-83&fromPageDetails=true&collapse=true&ycord=329 (accessed April 5, 2013).

United States Code. 2012c. 50 USC 9-response to threats of terrorist used of WMD. http://policy.defense.gov/portals/11/Documents/hdasa/references/50%20USC%202311.pdf (accessed April 5, 2013).

US Army 20th Support Command. 2011. 20th support command CBRNE.

US Army Chemical Materials Activity. 2012. Storage. http://www.cma.army.mil/aboutcma.aspx (accessed December 3, 2012).

US Army Intelligence. 2013. Army Intelligence vision and mission. http://www.dami.army.pentagon.mil/ (accessed April 9, 2013).

US Army Research, Development and Engineering Command. 2013a. Mission and intent. http://www.army.mil/article/39385/ (accessed April 2, 2013).

US Army Research, Development and Engineering Command. 2013b. Edgewood Chemical Biological Center. https://www.ecbc.army.mil/about/index.html (accessed April 2, 2013).

US Army Special Operations Command. 2013a. United States special operations command. http://www.soc.mil/USASOC%20Headquarters/USASOC%20Headquarters.html (accessed April 13, 2013).

US Army Special Operations Command. 2013b. USASOC fact sheet. http://www.soc.mil/UNS/Fact%20Sheets/USASOC%20Fact%20Sheet.html (accessed April 13, 2013).

US Central Intelligence Agency. 2007. CSI: Definition of intelligence analysis. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_1.htm (accessed February 1, 2013).

US Central Intelligence Agency. 2010a. The intelligence cycle. https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html (accessed October 2, 2010).

US Central Intelligence Agency. 2010b. System model of the intelligence cycle. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/page_52.pdf (accessed October 2, 2010).

US Central Intelligence Agency. 2013. CIA mission. https://www.cia.gov/index.html (accessed April 9, 2013).

US Coast Guard. 2010. Intelligence. http://www.uscg.mil/doctrine/CGPub/CG_Pub_2_0.pdf (accessed April 9, 2013).

US Defense Intelligence Agency. 2011. 2012–2017 defense intelligence agency strategy. http://www.dyn-intl.com/media/19969/the_defense_intelligence_agency_strategic_plan.pdf (accessed February 1, 2013).

US Defense Intelligence Agency. 2013. Mission. http://www.dia.mil/ (accessed April 9, 2013).

US Department of Defense. 1993. Department of Defense directive 3025.1. http://www.acq.osd.mil/cp/dodd/dodd_3025.1.pdf (accessed April 9, 2013).

US Department of Defense. 1994. Manual for civil emergencies. http://www.iaff.org/hs/disasterrelief/resources/ManualForCivilEmergencies.pdf (accessed April 14, 2013).

US Department of Defense. 1997. Department of Defense directive 3025.15. http://www.cdmha.org/toolkit/cdmha-rltk/PUBLICATIONS/dodd3025_15.pdf (accessed April 14, 2013).

US Department of Defense. 2003. The DoD role in homeland security. http://www.ndu.edu/uchs/ndaa%20fy02%20report%20%28dod%20in%20hs%29%20-%20final.pdf (accessed April 2, 2013).

US Department of Defense. 2012. 50 USC response to threats of terrorist use of WMD. http://policy.defense.gov/portals/11/Documents/hdasa/references/50%20USC%202311.pdf (accessed April 5, 2013).

US Department of Defense. 2013. Defense intelligence. http://www.defense.gov/home/features/2013/0113_defense-intelligence/ (accessed February 1, 2013).

US Department of Homeland Security. 2006. DHS intelligence enterprise strategic plan. http://www.fas.org/irp/agency/dhs/stratplan.pdf (accessed October 16, 2010).

US Department of Homeland Security. 2008a. Information sharing strategy. http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf (accessed October 23, 2010).

US Department of Homeland Security. 2008b. *Safeguarding Information Designated As Chemical-Terrorism Vulnerability Information (CVI)*, Revised Procedural Manual.

US Department of Homeland Security. 2013. About the office of intelligence and analysis. http://www.dhs.gov/about-office-intelligence-and-analysis (accessed April 9, 2013).

US Department of Justice. 2000. Department of Justice facsimile, Posse Comitatus.

US Department of State. 2013. Bureau of Intelligence and Research. http://www.state.gov/s/inr/ (accessed April 9, 2013).

US Department of the Army. 2009. CARA-West mission is varied, dangerous at times. http://www.army.mil/article/26089/cara-west-mission-is-varied-dangerous-at-times/ (accessed April 4, 2013).

US Department of the Army. 2012. ADP 2-0: Intelligence. http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adp2_0.pdf (accessed February 17, 2013).

US Department of the Army. 2013. 20th support command. http://www.army.mil/20thcbrne (accessed April 2, 2013).

US Department of the Treasury. 2012. Nonproliferation: What you need to know about treasury restrictions. http://www.treasury.gov/resource-center/sanctions/Programs/Documents/wmd.pdf (accessed February 18, 2013).

US Department of the Treasury. 2013. Terrorism and financial intelligence. http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Intelligence-Analysis.aspx (accessed April 9, 2013).

US Federal Emergency Management Agency. 2013a. National planning frameworks. http://www.fema.gov/national-planning-frameworks (accessed May 13, 2013).

US Federal Emergency Management Agency. 2013b. Mission areas. http://www.fema.gov/mission-areas (accessed May 13, 2013).

US Federal Emergency Management Agency. 2013c. National preparedness goal. http://www.fema.gov/national-preparedness-goal (accessed May 13, 2013).

US Federal Emergency Management Agency. 2013d. Core capabilities. http://www.fema.gov/core-capabilities (accessed May 13, 2013).

US Government Accountability Office. 2010. Iran sanctions: Complete and timely licensing data needed to strengthen enforcement of export restrictions. http://www.gao.gov/new.items/d10375.pdf (accessed January 5, 2013).

US Government Accountability Office. 2011. Intelligence, surveillance, and reconnaissance: Actions are needed to increase integration and efficiencies of DoD's ISR enterprise. http://www.gao.gov/products/GAO-11–465 (accessed February 12, 2012).

US Intelligence Community. 2008. Information sharing strategy. http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf (accessed October 22, 2010).

US Joint and National Intelligence. 2012. Joint publication 2001: Joint and national intelligence support to military operations. http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf (accessed December 12, 2012).

US Joint Chiefs of Staff. 2005. Homeland security, joint publication 3-26. http://dmna.ny.gov/plans_training/j5/General%20Interest/Selected%20Joint%20Pubs/JP_3–26_Homeland_Security_Aug_05.pdf (accessed April 10, 2013).

US Joint Chiefs of Staff. 2009. Combating weapons of mass destruction, joint publication 3-40. http://www.dtic.mil/doctrine/new_pubs/jp3_40.pdf (accessed April 10, 2013).

US Joint Chiefs of Staff. 2012. Chemical, biological, radiological, and nuclear consequence management, joint publication 3-41. http://www.dtic.mil/doctrine/new_pubs/jp3_41.pdf (accessed April 10, 2013).

US Marine Corps. 2013. USMC Intelligence Department mission. http://www.hqmc.marines.mil/intelligence/UnitHome.aspx (accessed April 9, 2013).

US Naval War College. 1992. *Sound Military Decision*. Naval Institute Press, Annapolis, MD. (Originally published in 1942 by the US Naval War College).

US Northern Command. 2013a. About NORTHCOM. http://www.northcom.mil/About/index.html (accessed April 10, 2013).

US Northern Command. 2013b. The Posse Comitatus Act. http://www.northcom.mil/About/history_education/posse.html (accessed April 2, 2013).

US White House. 2011. Presidential Policy Directive 8. http://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf (accessed April 14, 2013).

Chapter 8

Preparedness, Preventive, and Defensive Measures

8.1 Introduction

This chapter introduces the emergency preparedness and response before or in the event of a disaster or terrorist attack on pipelines, tunnels, and underground rail and transit systems. Some features to aid the detection of clandestine tunnels, illegal manpower mobilization for transshipment, fabrications of weapons of mass destructions (WMD), and improvised explosive devices (IEDs) will be presented in this chapter. Clever techniques for the detection and deactivation of land mines and IEDs using intelligent improvised technologies with *Mother Nature* support as meteorological and environmental modifications will be discussed briefly in this chapter to protect homeland, to safeguard infrastructures, and to defend law enforcement and military men.

This chapter is mainly an extension of Chapter 10 based on the book entitled *Risk Assessment for Water Infrastructure Safety and Security*, 2011, for the emergency preparedness, response, and preventive measures from Sections 8.1 through 8.7 for oil and gas pipelines, mine tunnels, road/highway tunnels, freight transportation by tube and capsule pipelines (e.g., *CargoCap*), underground high-speed transportation systems (i.e., *magnetic levitation train*), underwater tunnel, high-speed and trackless rail (e.g., *tubular rail*), and transit systems, including other assets.

8.2 National Response Framework

The US Department of Homeland Security (DHS) developed the National Response Framework (NRF) to conduct all-hazards response in the United States (FEMA 2008). The NRF is a guide to how the federal, state, local, and tribal governments, along with nongovernmental and private sector entities, can collectively respond to and recover from all disasters, particularly catastrophic disasters such as Hurricane Katrina, regardless of their cause (GAO 2008). The NRF recognizes the need for collaboration among the myriad of entities and personnel involved in response efforts at all levels of government, nonprofit organizations, and the private sector (GAO 2008). Hence, the overall guidelines of the NRF are in accordance with the National Incident Management System (NIMS), which offers a systematic standard for managing incidents. The second edition of the NRF was released in May 2013 and can be accessed on the Federal Emergency Management Agency (FEMA) website (http://www.fema.gov/national-response-framework). The new NRF incorporates a focus on the whole community and its core capabilities (FEMA 2013). The revised National Response Framework (FEMA 2013)

- Has a modified structure that is consistent with the other National Planning Frameworks released in 2013
- Incorporates the "whole community" term and concept; the concept is consistent with 2008 NRF but was not called "whole community" until the revision
- Recognizes families, individuals, and households as the main components of the whole community; the Framework has a section to describe their roles and responsibilities and incorporates related activities and coordinating structures
- Features the core capabilities aligned to the response mission area and provides definitions, critical tasks, and examples of organizations that deliver each capability
- Identifies the emergency support functions (ESFs) as the primary federal coordinating structure for delivering response core capabilities; the 2008 NRF included ESFs but did not formally recognize them as coordinating structures
- Has removed the planning chapter from the existing NRF, as it will have a more appropriate home in the new Response Federal Interagency Operational Plan (FIOP); the revised NRF briefly discusses planning and refers to the FIOP
- Has removed the recovery section, as the content now resides in the National Disaster Recovery Framework, released in 2011
- Has removed the descriptions of positions and responsibilities at the field support structure level, as they will be covered in the Response FIOP
- Places greater emphasis on the role of federal agencies in non-Stafford Act incidents

8.2.1 Local Governments

Local governments, departments (e.g., emergency medical services, police, fire, emergency management, and public works), and volunteers are usually the first to respond to incidental threats or hazards. The responsibility of the locally appointed official is to ensure public safety and welfare, to organize plans, and to integrate their capabilities and resources with neighboring jurisdictions.

8.2.1.1 Roles of Chief Elected or Appointed Officials

Elected officials provide direction and guidance to constituents during an incident and help modify regulatory requirements and budgets for preparedness efforts, emergency management, and response plans. However, they do not regularly focus on emergency management and response efforts.

8.2.1.2 Roles of Emergency Managers

The emergency manager mainly integrates the local emergency management program and evaluates the availability of local resources needed during an incident. Other objectives and missions of the local emergency manager include the following: (1) coordinating, planning, and working cooperatively with other local agencies and private sectors; (2) establishing common aid and support agreements; (3) facilitating damage assessments during incidents; (4) advising local officials about emergency management actions during disaster and terrorism incidents; (5) providing public awareness, standard training procedures, and education programs; (6) conducting exercises to examine plans and employ evaluation; and (7) including the private sector and nongovernmental organizations (NGOs) in planning, training, exercises, and evaluation.

8.2.1.3 Roles of Department and Agency Heads

Department and agency heads are responsible to work with the emergency manager in developing local emergency standard plans and procedures to ensure public safety and security. For instance, the US Environmental Protection Agency (USEPA) and local water agencies coordinate with emergency managers in preparing emergency response plans to ensure public health protection in the event of contamination or when the drinking water supply is determined to be a potential hazard.

8.2.1.4 Roles of Individuals and Households

Individuals and households should be informed and educated regarding their roles in the overall emergency management strategy. They can make a big difference

by preparing supplies, emergency kits, and plans for disaster and terrorism. It is obviously very difficult to make every house and individual develop emergency plans for themselves, while their focus is to survive in these current economic situations. The local government such as that of the county or city should provide standard household emergency plans and provide programs to systematically remind every individual and household to be prepared in advance for an unwanted event such as a disaster or terrorism. They can also be persuaded to be volunteers in response and recovery operations with an established voluntary agency. The local government may provide credits to individuals who allow themselves to be part of emergency response training courses, as this may encourage them to be more devoted volunteers.

8.2.2 States, Territories, and Tribal Governments

State, territory, and tribal governments have sovereign rights; unique factors are involved in working with these entities. Stafford Act assistance is available to states and Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands, which are included in the definition of "State" in the Stafford Act (FEMA 2008a).

8.2.2.1 Roles of the Governor

The governor is responsible for activating the state resources and implementing the strategic protocols needed for different kinds of incidents. Moreover, in accordance with state law, the governor has controls over certain orders or regulations associated with response. The governor's roles based on the NRF include but are not limited to the following: (1) communicating and helping the public to cope with the unwanted consequences; (2) commanding the state military forces (not in federal service and state militias); (3) facilitating emergency aid from other states under interstate mutual aid and assistance agreements; (4) seeking federal support under the Stafford Act presidential declaration of an emergency when resources are determined to be insufficient; and (5) working together with affected tribal governments within the state and initiating requests for the Stafford Act presidential declaration of an emergency on behalf of the affected tribe when needed.

8.2.2.2 Roles of the State Homeland Security Adviser

The state homeland security adviser provides counseling and guidance to the governor on homeland security issues and may serve as a liaison between the governor's office, the state homeland security structure, the DHS, and other organizations both inside and outside the state (FEMA 2008a).

8.2.2.3 Roles of the Director of the State Emergency Management Agency

The director of the state emergency management agency safeguards the state by providing preparedness actions to deal with large-scale disaster and terrorism emergencies, aids local governments, and provides emergency assistance with other states and the federal government. If local resources are determined to be insufficient, officials can request additional support from the county emergency manager or the state director of emergency management. For example, USEPA may assess or prevent water contamination without waiting for requests from state, tribal, or local officials.

8.2.2.4 Roles of Other State Departments and Agencies

State department and agency leaders together with their staffs develop, plan, and train internal policies and procedures to meet response and recovery needs safely. They should be involved in interagency training and exercises to enhance and polish the necessary capabilities.

8.2.2.5 Roles of Indian Tribes

The United States has a trust relationship with Indian tribes and recognizes their right to self-government. The state governor usually requests a presidential declaration representing the tribe to seek assistance from the state or the federal government under the Stafford Act, when local resources are inadequate.

8.2.2.6 Roles of Tribal Leaders

The tribal leader ensures the safety and welfare of the people of that tribe. As authorized by the tribal government, the tribal leader (1) is responsible for coordinating tribal resources needed for preparedness, mitigation programs, and emergency management from disaster and terrorism incidents; (2) may have powers to amend or suspend certain tribal laws; (3) can request federal assistance under the Stafford Act through the governor of the state when the tribe's capabilities and resources are found to be insufficient; and (4) can deal directly with the federal government under the Stafford Act through the state governor's assistance.

8.2.3 Federal Government

The president has the authority to command the federal government to take action for federal disaster assistance to large-scale disaster and terrorism incidents under presidential declarations and the Stafford Act. According to the DHS (2008), when the overall coordination of federal response activities is required, it is implemented

through the secretary of homeland security consistent with Homeland Security Presidential Directive 5 (HSPD-5).

8.2.3.1 Role of the Secretary of Homeland Security

The secretary of homeland security provides the president with an overall systematic pattern for domestic incident management, to coordinate the federal response with the support of other federal partners. The Federal Emergency Management Agency (FEMA) administrator, as the principal adviser to the president, the secretary, and the Homeland Security Council on all issues regarding emergency management, helps the secretary in meeting the HSPD-5 responsibilities (FEMA 2008a).

8.2.3.2 Law Enforcement

According to the DHS (2008), the attorney general has the leadership and authority for criminal investigations of terrorist acts in the United States or directed at US citizens or institutions in foreign countries, including the coordination of the law enforcement community and intelligence community to protect the homeland from terrorist attacks.

8.2.3.3 National Defense and Defense Support of Civil Authorities

As stated by the Office of the Under Secretary of Defense for Policy (OUSDP) (2010), the primary mission of the US Department of Defense (DoD) and its components is national defense. Because of this critical role, resources are committed only after approval by the secretary of defense or by the direction of the president (OUSDP 2010). Many DoD components and agencies are authorized to respond to emergency and to provide support. The provision of defense support is evaluated by its legality, lethality, risk, cost, appropriateness, and impact on readiness (OUSDP 2010).

8.2.3.4 International Coordination

According to the HSPD-5 (DHS 2008), the secretary of state provides leadership and management of international preparedness, response, and recovery actions for the protection of US citizens and US interests overseas.

8.2.3.5 Intelligence

According to the office of the director of national intelligence (DNI) (2007), the DNI or the director of the US intelligence community serves as the president's principal intelligence adviser, and oversees and directs the implementation of the National Intelligence Program.

8.2.3.6 Private Sector and Nongovernmental Organizations

The private sector and NGOs provide services in coordination with the governmental agencies and organizations in accordance with the NIMS principles. They are allowed to provide contingency plans and protocols.

8.2.3.7 Roles of Private Sector

Private sector organizations offer welfare and protection to their employees in the working environment. In addition, emergency managers must work with businesses that are entirely involved in critical infrastructure services (e.g., water, security, and power). The owners and operators of certain regulated infrastructures (e.g., petroleum refinery) may be legally accountable for preparedness and response actions to a negative incident that can occur. In the event of a disaster or terrorist attack, private sectors should be working together with the local emergency managers in the decision-making process to achieve an effective response and recovery operation.

8.2.3.8 Roles of Nongovernmental Organizations

NGOs offer temporary housing, provide immediate relief, support emergency food supplies, and undertake other services to assist the victims of the calamities. They usually coordinate with the government for supporting and planning the allocation of substantial resources.

8.2.3.9 Roles of Volunteers and Donors

Dedicated volunteers and donors can help response endeavors through different approaches, and it is essential that governments at all levels plan ahead to effectively incorporate volunteers and donated goods into their response activities.

8.3 Emergency Preparedness

Preparedness is a way of mitigating unwanted outcomes and it is one of the crucial actions in achieving safety and security in the event of calamities, disasters, and terrorism. This section presents the six essential activities for responding to an incident: (1) planning, (2) organization, (3) training, (4) equipment, (5) exercises, and (6) evaluation and improvement.

8.3.1 Planning

Effective planning includes the collection and analysis of information, policy and strategy formulations, plans, and other arrangements to operate missions and goals. It also sharpens the response operation by unequivocally defining required

capabilities, acquiring speed of action to take control of an incident, and facilitating the rapid exchange of information about the situation and event. Response plans have multiple things to address; for instance, evacuations face so many challenges. Therefore, systematic plans must incorporate the following: (1) the lead time required for various unexpected and anticipated events; (2) weather conditions; (3) transportation and communication; (4) interdependencies between locations of shelters and transportation (FEMA 2008b; US Army-CAC 2010); and (5) provisions of special needs populations and those with household pets (CRS 2010).

8.3.2 Organization

According to FEMA (2004), NIMS provides standard command and management structures pertaining to response. This standardized approach allows responders from different disciplines to collectively operate to respond. Government agencies and other organizations shall operate an emergency response in accordance with NIMS organizational and management policy.

8.3.3 Equipment

According to FEMA (2008a), the local, tribal, state, and federal jurisdictions need to establish a common understanding of the capabilities of different types of response equipment. A critical component of preparedness is the acquisition of equipment that will perform according to established standards, including the capability to be interoperable with equipment used by other jurisdictions and participating organizations (FEMA 2004). Efficient preparedness operations need standards to define techniques and create strategies to acquire and direct resources and appropriate equipment in sufficient quantities to accomplish assigned missions and goals. The federal government and local governmental agencies should ensure that their personnel have the necessary resources to perform assigned response missions and tasks.

8.3.4 Training

Training methods shall be in accordance with the standards of FEMA and produce qualified skills and proficiency. FEMA as well as other governmental and private organizations offer response and incident management training in online and classroom formats.

8.3.5 Exercises, Evaluation, and Improvement

Well-organized exercises improve interagency coordination and communications, enhance proficiency, sharpen skills, and determine opportunities for advancement

or expansion. Exercises should include but not be limited to the following: (1) include multidisciplinary, multijurisdictional incidents; (2) integrate involvement of academia, private sector, and NGOs (including international organizations); (3) refine aspects of preparedness processes, procedures, and plans; and (4) contain a system for integrating remedial actions.

8.4 Response

Emergency response is an action and operation of activating the society's resources and capabilities to save and safeguard lives; securing assets and the environment from irreversible damages; maintaining public morale and confidence; preserving social, economic, and political structure of the jurisdiction. The key actions usually involve in support of a response: (1) progress and maintain awareness to every situation, condition, and event; (2) activate and deploy key resources and capabilities; (3) effectively and efficiently coordinate response actions; and (4) demobilize.

8.4.1 Baseline Priorities

Situational attentiveness requires systematic screening of potential sources of information and detailed evaluation of the information should be employed. Critical information is directed through orderly reporting systems. Priorities include (1) providing appropriate plausible and precise information at the right time; (2) enhancing and expanding the national reporting system; and (3) involving operations centers and experts.

8.4.2 Local, Tribal, and State Actions

Local, tribal, and state governments can address the inherent challenges in establishing successful information-sharing networks by (1) creating fusion centers that integrate agencies associated with homeland security, academia, intelligence, emergency management, public health, and other agencies, as well as private sector and NGOs locally and "internationally," to expand the information-sharing strategy; (2) implementing the National Information Sharing Guidelines to improve intelligence; (3) establishing information-sharing and reporting protocols to enable effective and timely decision making during response to incidents; and (4) developing standard procedures that can provide awareness to misleading information that can cause distortion of intelligence. The local or regional Joint Terrorism Task Force should be informed immediately when a potential terrorist attack is detected.

8.4.3 Federal Actions

The National Operations Center (NOC) is responsible for collecting, assessing, and synthesizing all-source information, across all-threats and all-hazards information comprising the range of homeland security partners. Information regarding actual or potential terrorism and disaster incidents should be reported immediately by federal departments and agencies.

8.4.4 Alerts

When notified of a threat or an incident that potentially requires a coordinated federal response, the NOC analyzes and assesses the information before it goes to the senior federal officials and federal operations centers: the National Response Coordination Center (NRCC), the FBI SIOC, the NCTC, and the National Military Command Center, to assist them in creating effective decision making. Once the information is verified and processed, the secretary of homeland security coordinates with other appropriate departments and agencies to initiate emergency plans in accordance with the *framework*. Government and agency officials should often be aware and prepared to participate in all situations (through video and teleconference). Each federal department and agency must ensure that its response personnel are knowledgeable, well-prepared, and well-trained to utilize these tools.

8.4.5 Operations Center

Federal operations centers are essentially involved in awareness of circumstances, current events, and communications among governmental offices all over the nation. These operations centers can provide information, assistance, and guidance, and administer resources with their state, tribal, and local partners in the event of an incident.

8.5 Activate and Deploy Resources

According to FEMA (2008a), when an incident or potential incident occurs, responders assess the situation, identify and prioritize requirements, and activate available resources and capabilities to save lives, protect property and the environment, and meet basic human needs. Usually, this includes development of incident management objectives based on incident management priorities, development of an incident management action plan by the incident management command in the field, and development of support plans by the appropriate local, tribal, state, and/or federal government entities. The key activities include activating people, teams, resources, and capabilities based on the scope, capacity, nature, and complexity of the incident. All emergency responders should frequently exercise notification systems and protocols.

8.6 Proactive Response to Catastrophic Incidents

Prior to catastrophic incidents, state and federal governments should create models of detailed terrorism and disaster activity scenarios qualitatively and quantitatively equivalent to the combat zones presented in Chapter 7. Then, they should take proactive actions to mobilize assets in anticipation of a formal request from the state for federal assistance. They should not wait until some minor or major unfavorable events take place. Such deployment of federal assets would likely occur for catastrophic events involving terror threats, disasters, or high-yield explosive WMD or other catastrophic incidents affecting heavily populated areas. The *proactive responses* are used to ensure that resources are sufficient and reach the scene in a timely manner to assist in restoring normal function of state or local governments.

8.7 Recovery

Once immediate lifesaving operations are accomplished, the focus changes to assisting the critical infrastructures involved in the incidents and recovery. Within recovery, actions are taken to help the public and the nation return to normal condition. Depending on the complexity of this level, recovery and remediation efforts involve significant contributions from all sectors of our society.

8.8 Preventive and Defensive Measures

Preventive and defensive measures are presented in the following sections. Employment of these measures would improve the protection of pipelines, tunnels, underground rail and transit operations, and homeland.

8.8.1 Oil and Gas Pipeline Protection

Oil and gas pipelines including other energy resource distribution systems should be secured. Most of the security approaches for pipelines are focused on personnel safety and intrusion detection within the plant facility but not on protecting pipeline infrastructures. For instance, security at the trans-Alaska pipeline during the Gulf War included measures such as armed guards, controlled access, intrusion detection, and dedicated communications at key facilities, as well as aerial and ground surveillance of the pipeline corridor (GAO 1991). However, the events of September 11, 2001, and the pipeline terrorism in the Middle East influenced stakeholders and owners regarding pipeline system protection. According to the American Gas Association (AGA 2002), companies strengthened emergency, contingency, and business continuity plans; increased

their liaison with law enforcement; increased monitoring of visitors and vehicles on pipeline property; monitored pipeline flows and pressure on a continuous basis; increased employee awareness to security concerns; and deployed additional security personnel. The industry also began developing encryption protocol standards to protect gas systems from cyber attack (Ryan 2002). However, security is not enough to stop terrorist groups and disgruntled individuals from tampering or destroying pipeline infrastructures. Technological defensive methods are vital to deter and defend terrorists from sabotaging pipeline infrastructures.

8.8.2 Road, Highway, and Rail Tunnel Protection

Road, highway, and rail (RHR) tunnel systems design normally incorporating environmental safety and are designed to withstand structural loads and stresses and accidents but not terrorist or WMD attacks. For instance, subterranean tunnels are built with water evacuation and safety systems to move air into and out of the tubes; they are also built with fire evacuation systems. A transportation tunnel is designed and constructed to endure pressures and strains within the soil, riverbed, or seabed. Regardless of these safety measures, terrorism to tunnels can negatively impact their structural integrity and operations or lead to severe damage of the tunnel to the point that it becomes dysfunctional. The following sections will present different types of preventive measures and emergency responses.

8.8.2.1 Fire and Emergency Response

Based on the response levels of first responders to a given emergency situation, environment, or hazardous condition, the following groups are representative of classification of departments and agencies based on their function by various governments: (1) law enforcement; (2) fire services; (3) emergency medical services; (4) emergency management; (5) HAZMAT team; (6) explosives team; and (7) search and rescue (Radvanovsky and McDougall 2010). Firefighters and law enforcement personnel are typically the first groups to respond to accidents (e.g., HAZMAT spills and automobile accidents) and terrorism, as responding to such events requires skills appropriate to the nature of the events. An example of a transit system incident is the Moscow Metro terrorism in 2010 in which 40 people were killed and more than 100 people injured. Another example is that of a suicide bomber who detonated bombs during the morning rush hours at the Moscow metro (Avtozavodskaya station's green line) that killed 41 people and injured 120. Additionally, 700 people had to be evacuated from the station. There were events of confusion and panic as hundreds of people fled the explosion. Firefighters, law enforcement personnel, and the emergency response team responded to the incident. Scattered legs, arms, and other body parts in addition

to dead bodies were strewn around and in the train. Hazardous debris and fragments remained at the site. Traffic was rerouted and thus created temporary chaos in the surrounding area. Law enforcement personnel assisted the public to regulate the streets, minimize chaos, and halt all movement in the subway.

8.8.2.2 Preventive Systems for Road and Highway Tunnels

The countermeasures can be grouped into four categories:

1. Minimum level protection measures
2. Measures for an elevated threat level (ETL)
3. Permanent protection improvements (PPI)
4. Defensive measures

These categories were developed based on the current state of practice, the current method of physical security for transportation systems by other experts, structural weaknesses of tunnel structures and systems, and the defensive systems based on the result from the risk analysis in Chapter 7.

8.8.2.2.1 Minimum Protection Level

Minimum protection level (MPL) means *current temporary and permanent operational measures that have already been adopted*. These protection systems, likely required by the local government code and/or widely accepted by professional organization standard design and practice for tunnel and transportation safety and security, should already be recommended by other experts. These MPL measures include the following:

1. Lighting and emergency lines
2. Ventilation system
3. Smoke and fire detection system
4. Fire protection system
5. Fire emergency system
6. Emergency exit exercises
7. Closed-circuit television (CCTV) system
8. Closed-circuit video equipment (CCVE)
9. Security awareness training to personnel
10. Roving patrols
11. HAZMAT restrictions
12. Background checks to personnel
13. Access controls
14. Tunnel/transportation personnel identification system
15. Intrusion detection system to secured areas

16. Evacuation procedures
17. Procedures for rerouting of transportation to safer directions
18. Procedures for regulating public chaos and directing public to safer areas
19. Procedures to temporarily halt rail and transit operations
20. Extend/heighten supply air intakes
21. Cyber and information security
22. Backup manual for control of systems
23. Regularly scheduled data backup
24. Full-scale emergency response exercises

8.8.2.2.2 Measures for an Elevated Threat Level

ETL preventive measures are operational measures only employed during high-level terrorism events in a tunnel and its facilities. The verifications of the credibility of ETL are usually done by local and/or national-level intelligence agency and local law enforcement, and the information will be forwarded to the tunnel stakeholders, owner, and operator. These ETL measures include immediate deployment of personnel-specific actions, law enforcement personnel, and may include the initiation of military support. The costs are dependent on the type of incident. Managers may consider possible scenarios to estimate the type of preventive measures applicable to an asset. These ETL measures include the following:

1. Security guards at portals
2. Inspection procedures for weapons and explosives materials
3. Explosive-sniffing dogs and other weapon detection systems
4. Onsite background checks
5. Waterborne patrols
6. Transshipment tracking protocols
7. WMD detectors
8. Video surveillance
9. Military response and support to law enforcement civilian

8.8.2.2.3 Permanent Protection Improvements

PPIs include the structural and system alterations of the tunnel including the surrounding area (i.e., safety encroachment), which should be added to optimize the safety and security of the tunnel. Implementing PPIs is more costly due to the inclusion of safety, security, and defensive measures, which require a lot of time, into risk assessment, engineering design, and construction. However, for existing tunnels, two only need to consider installing defensive systems and implement safety encroachment (if there is extra land available).

For high-speed transport technologies such as the underground maglev transport system (e.g., Swissmetro), underwater/immersed tunnels, and other underground freight transportation through pipeline systems should have layered security and defensive measures because they are costly to build and it requires a significant amount of time and effort to receive approvals for these infrastructures during preliminary development. Likewise, tubular rail transportation mainly requires defensive systems and safety distance. PPIs will not only provide safety and security for the tunnel systems but will also increase their functional and operational life, which could tremendously minimize future costs. PPIs include but are not limited to the following:

1. Safety encroachment for security and possible debris and missile burst during accidents or attacks
2. Safety emergency shelter from fragment and missile burst and other types of man-made disasters (only needed in overpopulated areas)
3. Intelligent devices to immediately deter and attack individuals carrying explosives (detection will be designed within a safety encroachment)
4. Explosive detectors
5. WMD detector (only needed in certain conditions)
6. Security and defensive systems for SCADA and cyber technology
7. Redundant ventilation systems (RUS)
8. Redundant power supply
9. Redundant columns
10. Interior liner steel panels
11. Interior concrete panels
12. Interior and exterior concrete grouting
13. Interior liner bolting or tiebacks
14. Emergency floodgates (prevent floods created by a disaster or terrorism)
15. Precast concrete slab over tunnel
16. Interior and exterior roof steel plates
17. Control access using fencing and bollards connected to intelligent detection and defensive devices
18. Concrete encasement of columns
19. Reinforced fiber protection wrapping of columns
20. Steel jacketing of columns

8.8.2.3 Preventive Measures for Terrorism

Most preventive measures presented here are directed toward disaster created by terrorism because, typically, the engineering of tunnel systems already considers earthquake loads and other natural hazards based on the areas. However, terrorism has not been factored into the engineering design of tunnel and transportation systems.

8.8.2.3.1 Effectiveness and Cost

The effectiveness and cost of preventive measures in terms of both physical and operational measures can be assessed using risk acceptability analysis (refer to Chapters 6 and 7), where an expert has to consider alternatives comparing the strength and effectiveness of technology, policy, strategy, and operation for the controllability of risks of terrorism.

Physical measures require planning, design, permits, construction, regular inspection, and maintenance to retain excellent performance. Operational measures involve operators or personnel for security, safety, and defense. If there are no policies enforcing the use of new preventive measures and defensive systems, then the policies required should be developed and implemented.

There are four categories of strategies under preventive measures:

1. *Deterrence*—a strategy to disrupt terrorists from destroying an asset. It should begin with regulations requiring stakeholders, owners, and/or operators to comply. For instance, the regulations should require safety encroachment or safety shelter in overpopulated areas near transit facilities. The owner or operator should develop an inspection policy for public safety as per regulations. Natural disasters can only be avoided (refer to Chapter 6, Section 6.1.1.5, *Avoidability of Risks*). Another way to deter terrorists from disrupting an asset's operation is to install a sophisticated fence which can deter and defeat the enemy.
2. *Detection*—once the regulations are developed and implemented to enforce owners and operators to utilize inspection and technology for the detection of intruders, a threat can be detected using these new or existing technologies. Suicide bombers are hard to detect, especially in overpopulated areas; however, detection technologies can be designed to *discriminate* the bombers from the public. Explosive sensors can be installed on portals. To convince regulators to implement these types of sensors for railroads and railways is difficult because they are usually hundreds and thousands of miles long and situated in remote areas. The best way is to install detection systems on the train itself that can detect threats within certain distances, especially on those trains carrying classified and hazardous materials.
3. *Mitigation*—this involves strategic planning, procedures, and requiring security personnel/law enforcement team and/or firefighters to mitigate threats for sabotaging an asset. This requires effort for exercises, preparations, and systems synchronization. Plans for preparedness, response operations, agency mobilization, and other required preparedness protocols are really essential in this category. Planning for emergency exit of the public away from the incident and immediate rerouting of transportation and immediate information dissemination to other rail systems so they can be rerouted or halted even during the act of terrorism should be included to mitigate expansion of danger to the public.

4. *Defensive*—this category is not currently being implemented but should be a potential way to prevent terrorists from attacking assets, or creating mass casualties and severe injuries. A technological defensive system is really critical so that even before the terrorists with explosive devices can penetrate tunnel vicinities, they should be detected by intelligent devices and be defeated to the point of being destroyed immediately when carrying large-scale WMD. First, an intelligent device can be used to discriminate a potential threat from other individuals; when bombs are detected, the threat will be terminated if no other means are available to deter the individual's actions. This could be considered a lethal approach by regulators in the United States who may hesitate to implement this category, but if one has to protect hundreds or thousands of lives, this approach is one effective way to terminate the enemy.

8.8.2.4 Minimum Standard Preventive Measures

The following sections introduce and characterize in detail the common preventive measures for tunnels. In building and operating tunnel systems, safety is the primary consideration because of the complexity of emergency responses in the event of fatal accidents or terrorism. Part of safety approaches is to ensure clearances, ventilations, and safety shelter use for passengers during emergencies.

8.8.2.4.1 Basic Standard Preventive Measures: Lighting and Ventilation

Lighting provides visibility in the tunnel to personnel, emergency responders, and law enforcement officers, and surveillance videos can clearly record the occurrences in the tunnel during normal days and emergencies. Suspicious acts are seen immediately with the aid of lighting. The *ventilation system* in the tunnel is the most vital to public safety during disasters and accidents and even during normal operations. It can be designed depending on the characteristics of the tunnel such as the following:

- *Tunnel mode or usage*: highway, road, transit, mass transit, underwater, and capsule/tube freight system
- *Construction methodology*: immersed tube, cut-and-cover, bored or mined, and air-rights structures
- *Tunnel attributes*: length, shape, depth, occupancy loads, condition, and location
- *Date of initial construction*: very old tunnels dependent on the type of ventilation technology at the time of construction; however, it can be remodeled or replaced with available funding

8.8.2.4.2 Minimum Standard Preventive Measures: Roving Patrols

Roving patrols within the surroundings of subways, tubular rails, and underground high-speed rail and transportation system facilities improve security within those areas. Patrols should have access to monitor the surveillance camera from their automobiles. Highly skilled patrols should have the ability to control intelligent devices and defensive systems (if implemented) on their automobiles, especially for maglev trains carrying 500–800 passengers per transport system. They can immediately respond and perform during emergencies or when threats are detected by technological devices implanted near the facilities.

8.8.2.4.3 Minimum Standard Preventive Measures: Hazardous Material Surveillance and Security

Hazardous material (HAZMAT) surveillance is actually practiced by most transportation tunnel owners and operators to ensure that no illegal activities related to HAZMAT transshipments are carried out through rails and tunnels, avoiding the misuse of generating an explosion or contaminating the surrounding environment. This is standard operating procedure in most highway, road, and transit tunnels to protect public safety, assets, and the owners from liabilities. HAZMAT could be used by disgruntled or self-radicalized individuals or adversaries to create intentional accidents or spills. However, HAZMAT restrictions and inspections through tunnels could create delays to industries needing these materials.

8.8.2.4.4 Minimum Standard Preventive Measures: Background Investigation

Conducting background investigation of potential employees, vendors, and contractors is really important, particularly for those who have access to secured and sensitive facilities. This is basic practice to ensure that a possible employee has no criminal history or no extreme psychological disorders. Additionally, for personnel who access major control systems, there should be a random drug test.

8.8.2.4.5 Minimum Standard Preventive Measures: Access Controls

Access control policy and technology increase security to tunnel systems and secured facilities. Security fences, bollards, steel curtains, walls, and other types of barriers may be used to mitigate unauthorized persons from accessing secured facilities. Access controls can be defeated by stronger forces. However, fences should be integrated with other preventive measures such as detection, biometric, and alarm systems to detect intruders attempting to access the vicinity. There are five common types of concrete walls that are commonly used along the slopes:

1. *The gravity wall* must be designed based on gravity weight and soil mechanics to maintain stability, and should withstand tensile stresses.
2. *The semi-gravity wall* is a concrete wall that requires stronger vertical reinforcement from the footing to the upper end because it is thinner than the gravity wall.
3. *The cantilever wall* is a reinforced concrete wall with a base slab and a branch to structurally withstand the moments and shears.
4. *The counterfort wall* is similar to a retaining wall and is constructed with thin concrete slabs that are supported by vertical counterforts connected to the base footing intervals on the back of the wall.
5. *The crib wall* is designed similar to a gravity wall but is usually formed by rectangular cells stacked one on top of the other and filled with soil instead of using reinforced concrete.

8.8.2.4.6 Minimum Standard Preventive Measures: Employee Identification System

The employee identification system is a basic standard measure to avoid unauthorized employees from entering the tunnel facilities. It allows security personnel to validate every individual entering the facility, and it requires attentive tracking and identification maintenance to retain security standards. Identification devices should be installed in every secured area so that employees can be validated through the device before they are given permission for entry. Identification devices work well because identification cards can be deactivated if an employee no longer has permission to enter certain secured places.

8.8.2.4.7 Minimum Standard Preventive Measures: Evacuation Protocols

Evacuation protocols should be basic standard preventive measures in all types of tunnels for passengers and tunnel personnel in the event of fatal accidents and terrorism before the arrival of the law enforcement team and firefighters. Planning, risk management, and signage location plan are part of the evacuation protocols. Safety shelters and safety encroachment should also be included in the protocols to aid the public from exposure to fragment and missile bursts and toxic emission in the event of a disaster. The signage location plan shows pathways for safety evacuation, stairways, and safety shelters. Tunnel operators and personnel shall maintain up-to-date protocols and exercises.

8.8.2.5 High Standard Preventive Measures

One of the essential high standard preventive measures (HSPM) is the emergency response procedure, which should have exercises involving tunnel operators,

personnel, firefighters, the law enforcement team, and paramedics to cover all possible emergencies. Another very important preventive system for tunnels is the *emergency ventilation system (EVS) and redundant ventilation system (RVS)*, which will maintain a constant supply of fresh air, to protect the public from toxic substance, smoke, and emission of contaminated air during an incident in the tunnel. The minimum air velocity required for this ventilation system is approximately 2.0 m/s or below through open doors in the emergency facility. Different conditions are considered when designing a safety or emergency facility to ensure the prevention of smoke (or toxic substance) penetration into the facility, and for regulating chaos during the incident; consideration of emergency human behavior situation in the tunnel emergency facility is also important due to the considerable length of the tunnel. Detailed analysis for the design of a rescue or emergency facility is essential due to the complexity involving train movement during an emergency, ventilation system for smoke emission and hazardous debris, operational emergency measures, aerodynamic effects of trains, and structural safety measures.

The aerodynamic effects of trains during an emergency situation can be determined before the opening of the tunnel. The rest of the HSPM are the following:

- Security enhancement at portals
- Strict checkpoints
- Security improvements at surrounding water bodies
- Strict freight and ship tracking systems
- Illegal ammunition and explosive detectors
- *Weapons of mass destruction detectors*, which include the detection of chemical, biological, radiological, and nuclear (CBRN) weapons
- *Rescue concept and operation*, which require special planning effort to ensure uniformity of actions within a given time frame for rescue in one railway facility and with other railway networks
- *Provision of emergency facilities*, which include the following: (1) emergency telephone, (2) video surveillance and loudspeaker system for announcements; (3) lighting system comparable to that of a station; (4) seating accommodations; (5) separate areas for the treatment of injured persons and for toilets; and food and water supply. Additionally, the following structural and technical measures are taken in the emergency station:
  1. *Special air ducts or bypass channels*—should be built near both ends of the emergency
  2. *The bypass channels are also used to bring air* from the nonincident tube in the refuge area
  3. *Fresh air supply for the occupants in the waiting area* is provided by special fans which are located in the firefighter access passages (local ventilation system)

8.8.3 System Protection Interoperability for Road, Highway, and Rail Tunnels

Tunnel system safety approach is the comprehensive employment of technology, engineering, risk management, and management tools to identify, analyze, and control threats within a designated amount of resources and time. These integrate all components as follows:

- *Risk management*—provides measurement and avoidance of risk, as well as risk management
- Directive and policy—provide guidance to system operation
- *Manpower mobilization*—ensures mobilization of tunnel personnel, the public, emergency responders, and vendors for operation, improvement, and maintenance
- *Operating procedures*—maintain routine operating and emergency procedures
- *Engineering and technology systems and controls*—maintain communication systems, emergency facility, safety encroachment ventilation systems, fences, intrusion detectors, lighting, fencing, explosive/WMD detectors, and defensive system
- Physical characteristics of the tunnel structure

8.8.3.1 Emergency Responders and Operating Procedures

Tunnel operators should maintain training programs which consist of the following: (1) *inherent hazards*, pedestrian/passenger traffic, transportation traffic, rail traffic, and traction power; (2) *ensure safety on right-of-way*; (3) *tunnel emergency systems*, ventilation, safety facility, hazardous debris protection, fire detection, fire suppression and hydrants, points of egress, and rescue areas; (4) *emergency communication systems*, billboards and telephones; and (5) *emergency protocols*. The public should be informed about security awareness and learn to identify threats and to report these suspicious acts to authorities.

Effective tunnel operations for safety and security can be achieved by providing comprehensive tunnel emergency response procedures that should include the following:

1. Reporting protocol
2. Information to be collected and evaluated
3. Verification and validation protocols
4. Protection of the area
5. Limiting vehicular and train traffic
6. Right-of-way safety
7. Transportation safety
8. Effects of bursting fragments, toxic debris, and missiles (impact on the rescue operation)
9. Effects of moving train during emergencies (aerodynamic effects of train)

10. Regulating public chaos (managing human behavior during emergencies)
11. Removal and restoration of traction power
12. Activation of emergency systems, including ventilation and dry standpipe system
13. Assistance in rescue and evacuation operations
14. Deployment of roving patrols
15. Posting of security guards
16. Explosive and WMD detection
17. Hazardous materials restrictions
18. Background investigations and verification of credentials
19. Inspections of vehicles, cargo/freight, and persons
20. Bomb-sniffing dogs
21. Command protocol
22. Information sharing (firefighters, law enforcement, security and defense agencies, and emergency medical services)
23. Military support operation
24. Defense readiness protocols

8.8.4 Engineering and Salient Features of Technological Systems

Fire protection, fire detection, threat detection technology (i.e., *using a technology capable of discriminating terrorists from passengers/public*), ventilation systems, lighting, fencing, barriers, WMD detection, and defensive approach (e.g., *an intelligent device is capable of discriminating and destroying a terrorist carrying explosives*) are examples of the engineering controls that support underground rail and transit systems and tunnel protection. These technological measures are used not only for disrupting a terrorist attack and aiding the detection of intruders but also to defend the infrastructure when explosives (e.g., suicide bombers) are detected.

8.9 Mine Tunnels Hazard Prevention

The following sections provide measures for mine tunnel hazard prevention.

8.9.1 Lighting in Mine Tunnels

Lighting installation for all underground mine tunnels is necessary for continuously maintaining safety operations. Mine tunnel owners and operators should provide and ensure lighting to critical locations as listed:

1. The entrance to each shaft, shaft landing station, and loading facilities
2. All areas where tunnel personnel and workers board transportation systems at the beginning and end of shifts

3. Underground machinery stations
4. Sidings, by-passes, and junctions
5. Areas where transportation is usually coupled or uncoupled
6. Major loading point for rail and mobile transport
7. First aid stations
8. Any place where lack of lighting may create a hazard

8.9.2 Emergency Supply Facilities

In every tunnel operation, first aid facilities should be provided:

1. First aid supplies should be installed in easily accessible areas at every given distance along the tunnel.
2. For every working shift (day shift and night shift), personnel with current and appropriate first aid certification or emergency response certificate should be available for support during emergencies.
3. Emergency rescue and shelter for an injured person.
4. Regular maintenance of first aid technology and supplies should be done.
5. Maintenance of an up-to-date emergency response plan and ensuring emergency exercises based on potential scenarios.

8.9.3 Thermal Stress

Thermal stress is one of the significant concerns in the underground environment or deep tunnels where it is difficult to maintain ventilation. Heat exhaustion can create fatal health injury to mine workers. Several workers die due to heat stroke. Therefore, first aid or emergency station, technology, and supplies are very important in this type of operation.

8.9.4 Access

Single access is inadequate when building a new mine tunnel (or new section). In the planning, a second means of egress in addition to the primary access should be planned prior to constructing the tunnel. A means of egress is an exit pathway that can be used for safety exit by workers. In a mine, a minimum of two means of egress are usually required. A safe and strong ladder or other types of safe tunnel operation methods must be installed in every shaft being sunk for workers and/or tunnel personnel ascending or descending.

8.9.5 Well-Being Monitoring

It is very important to monitor and inspect the health status of individuals working in a mine tunnel to detect any potential health hazard.

8.9.6 Training

Owners and operators of mine tunnels must require workers to undergo a training process which includes health and safety protocols, threat awareness, emergency response and preparedness, including supervision to perform competitive tasks and to avoid mistakes that can generate possible hazard. Vendors, visitors, and contractors who are at the site must also undergo basic training.

8.9.7 Personal Safety Devices and Accessories

Personal safety devices and accessories shall be provided to tunnel workers and personnel by owners and/or operators. Owners should enforce workers, contractors, and personnel to carry these safety gadgets, which they should be oriented and well trained to use properly and maintain, and should be responsible to inform owners or personnel when supplies are out. Owners should also have maintenance inspections for protective gadgets and supplies and provide updated manufacturer's equipment manuals to workers and personnel; these mandatory guidelines in the manual include but are not limited to the following:

1. Hard hat
2. Safety footwear
3. Hearing protection
4. Gas mask respirator
5. Eyewear and face protection
6. High visibility attire
7. Cap lamps and flash light with extra batteries
8. Oxygen, water, and food supplies (dry goods) for emergency use
9. Ready-to-use disposable packets of air-activated warmers for hand, toe, and body (these warmers typically emit heat for approximately 10 h per packet), rescue station
10. Ropes
11. Mini first aid kit
12. Waste disposal zip plastic bags for use when stranded in the tunnel
13. Mini-tracker and video (only needed when operating in very long and deep tunnels)
14. Communication devices for emergencies

8.9.8 Surface Area Boundary Planning and Design

Surface area boundary planning is a priority for rescue and emergency response in the event of hazards and accidents. The plans should detail and delineate the following:

- The boundaries of the surface area and/or limits of property lines

- All surface area infrastructures within the boundaries which include but are not limited to permanent and modular buildings, power poles or overhead lines, concentrators, workshops, explosive storage magazines, fuel location facilities, access roads, equipment storage facilities, maintenance facilities, assembly stations, and natural and man-made features (e.g., detention/retention ponds, wastewater treatment ponds, and drainage structures)
- All underground infrastructures and components including but not limited to buried and surface electrical services, high-voltage reticulation system, cable and communications lines, underground freight pipelines, gas lines, water lines, wastewater lines, tunnel entries, compressed air lines, and ventilation lines

8.9.9 Hazard, Vulnerability, and Risk Management of Mine Tunnels

The hazard, vulnerability, and risk management of mine tunnels should be continuously improved or updated and should include the following assessments and information:

1. Identification of potential and emerging hazards and associated risks
2. Assessment of the hazard and vulnerability including other possible threats
3. Determination of acceptable risks; to provide alternatives to maximize risk acceptability and minimize risk
4. Development of up-to-date preventive measures, and rescue and recovery plan
5. Recording, monitoring, and reviewing controls for effectiveness to maintain safety and security

Hazard, vulnerability, and risk management plans should reflect a hazard and risk management methodology as described in Chapters 5, 6, and 7 and should include but not be restricted to the following areas: (1) hazardous substances; (2) fire and explosion; (3) burst of missiles (fragments and debris); (4) spontaneous combustion; (5) inundation; (6) outburst/rockburst; (7) strata/lining failure; (8) release of hazardous substances; and (9) ventilation. The risks relating to each category must be determined as described and an assessment of the risk involved carried out in reference to Chapters 6 and 7. All hazard management plans dealing with identified risks and associated risks should be clearly documented and held on site for easy access. Each risk management plan should be inspected and reassessed annually as determined by the tunnel operator and risk manager. The hazard, vulnerability, and risk management plans should specifically define the roles, skill levels, and responsibilities of all personnel involved in implementation of regulations and procedures.

8.9.10 Hazardous Substances

Technological devices to monitor hazardous substance should be installed. Medical monitoring of hazardous substance exposure should be employed for workers, thus minimizing health injury.

8.9.11 Fire and Explosion

The tunnel operator and manager must ensure safety measures associated to underground explosion, flammable gas, and hazardous debris. Important considerations for the risk management plans are delineated as follows:

1. Remediation of incombustible dust roof, sides, and floor of accessible parts of the mine
2. Clean-up and prevention of dispersions/accumulations of coal dust that may contribute to an explosion or ignition of flammable gas
3. Employment and sustaining of explosion barriers
4. Provision of monitoring technology for the control of flammable and other explosive gases
5. Provision of adequate equipment for firefighting and resources for emergencies
6. Pre-ignition of explosives
7. Detection of flammability in the tunnels
8. Detection of hazardous gases
9. Water supply for firefighting purposes

8.9.12 Heating and Inundation

The owner or operator must ensure that a technology/equipment is in place to prevent spontaneous combustion in an underground coal mine and to mitigate any possible inundation into the tunnel. An inundation refers to an inflow of fluid material (i.e., water, flammable or noxious fluid). Important elements to consider are as follows:

1. To ensure effective risk management, the monitoring protocols applied must be reviewed annually. This is to provide systematic and standardized processes: (1) the nature of the risk assessment and management mechanism has not changed; and (2) the procedures that have been applied are adequate to manage risk.
2. The risk frequency monitoring and inspections based on the developed risk management should be recorded.
3. The risk assessment management plan must include the following:
   - Research, review actions, and evaluation of any available old plans, documents, and any other data and personnel with regard to dates, accuracy, verification, and validation

- Evaluation of any current data, reports, and personnel relevant to the inundation risk location
- Delineation of water bodies, former workings, aquifers, small dams, streams, ponds, or other systems likely to contain material capable of inundating the workings, and verification of the accuracy of the plans
- Compliance with federal and local codes and standards
- Include on-mine tunnel engineering plans all inundation preventive systems
- Barrier design and specification identifying purpose and location on the plan
- Failure of the geotechnical lining
- Reliability and safety of current tunnel engineering plans, verification, and approval
- Ventilation systems
- Safety shelter
- Provision and maintenance of adequate equipment and supplies for breaking into or working in close proximity to inundation risk areas
- Well-trained, experienced, and certified personnel
- Necessary documentation

8.9.13 Outburst and Rockburst

During the preliminary exploration phase and risk assessment process, the outburst and rockburst in mine tunnels must be analyzed and calculated and should be reviewed to mitigate hazards. The elements to be considered in the analysis and planning include the following: (1) length and depth of tunnel; (2) geotechnical, geological, and hydrogeological characterizations; (3) review and risk analysis of the outburst/rockburst in comparison to the engineering tunnel plan and ventilation system; (4) in situ gas content of the coal; (5) maintenance procedures; (6) program for boreholes, flank, and direct protective drilling; (7) stress-relieving methods; (8) barrier specifications; (9) gas discharge methods; and (10) provision of necessary equipment and supplies to manage and predict risks.

8.9.14 Strata Control in Mine Tunnels

The tunnel operator and management personnel should establish a procedure to ensure the integrity of worked ground. Elements to consider in risk management of strata control are as follows:

1. Engineering design of extraction and excavation methods
2. Engineering design (structural and construction) and specifications of pillar and support
3. Maximum distance at which roadways can be built before support is installed
4. Provision of suitable equipment and construction supplies
5. Monitoring of the structural stability of all openings

6. Providing training to workers and personnel regarding engineering design principles, placement and removal of support, knowledge of specifications and support systems, and identification of indicators of change that may affect the structural stability of all openings
7. Documentation or report preparation of geological features that may affect the structural stability of all openings
8. Recording or reporting preparation of strata failures that had the potential to injure persons
9. Mine geology, hydrogeology, and hydrology
10. Providing engineering plans and construction specifications of the proposed drivage of roadways
11. Any individual must not enter into unsupported underground tunnel

8.9.15 Mine Tunnel Explosive Materials Handling

Mine tunnel explosive materials' risk management and procedures should be created and implemented which only approved and certified explosive personnel should be allowed to handle and be responsible for: (1) storage, transport, and preparation of explosives; (2) charging and initiation of explosives; (3) treatment of misfires; and (4) disposal of waste explosive materials.

8.9.16 Mine Tunnel Ventilation

The ventilation system in a mine tunnel is used to maintain fresh air circulation and dilute harmful substances in the underground environment. Generally, standards of mine tunnel define fresh air as follows: (1) not less than 20% by volume of oxygen; (2) contains no more than 1 ppm of aldehydes (as formaldehyde; CH_2O or HCHO); (3) shows a concentration of respirable quartz dust of not more than 2.0 mg/m^3 on a long-term exposure; (4) shows a concentration of respirable coal dust of not more than 3.0 mg/m^3 on long-term exposure; and (5) contains the following common gases in mine tunnel at the lowest practicable level and at no more than the following levels:

1. Carbon monoxide (CO; CAS Number 630-08-0) (8 h time limit = 25 ppm; short-term exposure limit = 200 ppm)
2. Carbon dioxide (CO_2; CAS Number 124-38-9) (8 h time limit = 5,000 ppm; short-term exposure limit = 30,000 ppm)
3. Hydrogen sulfide (H_2S; CAS Number 7783-06-4) (8 h time limit = 10 ppm; short-term exposure limit = 15 ppm)
4. Oxides of nitrogen (nitric oxide, NO; nitrogen dioxide, NO_2; and nitrous oxide, N_2O) (8 h time limit = 3 ppm; short-term exposure limit = 5 ppm)
5. Sulfur dioxide (SO_2; CAS Number 7446-09-5) (8 h time limit = 2 ppm; short-term exposure limit = 5 ppm)

The *National Institute for Occupational Safety and Health (NIOSH) Pocket Guide to Chemical Hazards* (can be accessed from the US agency—Centers for Disease Control and Prevention: *http://www.cdc.gov/niosh/npg/*) has been developed as a source of information on most chemicals for workers.

8.9.17 Mine Tunnel Ventilation System Planning

Mine tunnels should develop and implement *mine tunnel ventilation system management* and should practice the following: (1) documentation, supplies, and maintenance of fans and ventilation structures; (2) seals and protocols; (3) underground monitoring methods and systems for air flow and ventilation; (4) preventive measures for ignition of flammable gases; (5) remediation and control of coal dust; (6) spontaneous combustion management; (7) ventilation characterization, inspection, and design; and measurement and characterization of air flowing in underground tunnels as per the standards specified in Federal, State, and/or local government mining underground and tunnel regulations. To protect public health safety, it is important to maintain flow of fresh air to every working place.

8.9.18 Airways, Air Crossings, and Stoppings

Air leakage should be prevented by preparing an engineering design of the main intake and return of a tunnel. Materials that are used for stoppings and air-crossings in main airways of a mine must be nonflammable or noncombustible. A minimum of two doors should be built between an intake and return airway, so that when workers and machinery are going through one door, the other door can remain closed to mitigate or reduce air leakage.

8.9.19 Mine Tunnel Emergency Response: Fire Control and General Emergency Systems

There are two categories of mine tunnel emergency response: *fire control and general emergency response*. Every underground tunnel site must have an emergency management plan that should address the following:

- Emergencies the systems cover that are potentially to be encountered at the tunnel or associated surface facilities
- Evacuation and rescue of workers from affected areas
- First aid or medical supplies for the treatment and transport of sick or injured workers
- Implementation of up-to-date emergency response plans
- Emergency fire procedures
- Actions to be taken immediately by workers who first discover a fire
- Provision of suitable firefighting equipment and resources

- Training and exercise in the use of firefighting equipment and resources
- Installation of water storage and water supply usable for firefighting
- Inspection and maintenance of fire equipment and resources
- Compatibility of fire equipment and resources with local fire and mines rescue units
- Provision of safety shelters
- Provision of communication devices and maintenance of effective communications
- A minimum of two means of egress from each production/working area
- Workers should be familiar with the use of paths for evacuation and rescue
- Provision of lighting, signage, and markings to aid workers to see pathways and route for evacuation in the event of emergencies
- Provision of transport system and escape alternatives to workers
- Posting a competent worker on duty on the surface with effective communication gadgets when anyone is in the tunnel
- Provision of methods or procedures to ensure closing of the tunnel or section of the tunnel during fire emergencies and other incidents

The fire control and emergency response procedures should be documented or a detailed report prepared, reviewed, and tested in a live or actual exercise annually, and a review of the entire system should occur every 2 years.

8.10 Approaches for the Detection of Illegal Tunnels by Other Experts

The surface of the earth has been mapped and mastered with lidar, photography, infrared, and other now-familiar systems, on satellites, manned aircraft, and drones (Roston 2013). Thermal imagers can even penetrate thin layers of soil, but how can one see inside solid ground, below the roads, the rocks, and the desert sand (Roston 2013)? This is a hot topic in US government research. Tunnels have bedeviled prisons, security forces, and border agents for years. Last summer, authorities discovered a 240-yard drug tunnel, fitted with electricity, lights, and a ventilation system, under Arizona's border with Mexico (Roston 2013). The previous year, there was embarrassing news from Kandahar: Almost 500 prisoners, including Taliban fighters, escaped from an Afghan prison via a 1000 ft tunnel (Roston 2013). Cross-border smuggling tunnels enable unmonitored movement of people, drugs, and weapons and pose a very serious threat to national security (Klar and Linker 2009). One of the focal points for research is the Rapid Reaction Tunnel Detection, a joint effort between the US Defense Department's Northern Command and the Department of Homeland Security's Science and Technology Directorate (Roston 2013). In 2006, an Israeli soldier was abducted in such a tunnel near the border between Israel and the Gaza Strip (Klar and Linker 2009).

In today's world, confronted with the realities of terrorism and terroristic objectives, one must also acknowledge that tunnels pose a looming threat to national security (Ugarte and Garcia-Olalla 2011). A 2007 operational need statement from the US Central Command (USCENTCOM) noted that detainees were attempting to build a tunnel as a means to escape from the internment facilities (Ugarte and Garcia-Olalla 2011). Another region with an emerging subterranean threat to US Forces is in Afghanistan with the Karez, or underground aquifers built to move irrigation water from mountains to villages by normal gravity-driven flow and present the Taliban and other insurgents with a means to cache weapons and materials, infiltrate and exfiltrate the battlefield, and move fighters and supplies (Ugarte and Garcia-Olalla 2011). Further, in Egypt, the flow of weapons, ammunition, and other contraband under the Egyptian border has contributed significantly to the ongoing Israeli–Palestinian conflict (Ugarte and Garcia-Olalla 2011).

Because illicit US cross-border tunnels are a departmental issue, the capabilities and strategies to counter this threat need to be developed jointly, optimized to meet departmental needs, and ensure unity of effort (DHS 2012). According to the DHS Office of the Inspector General, 2012, it is recommended that the Chief, US Border Patrol (DHS 2012):

- Conduct the planned study of how Customs and Border Patrol (CBP) can address tunnel detection capabilities through existing processes and procedures in support of the Analysis of Alternatives for the Tunnel Detection and Technology Program
- Complete the planned Concept of Operations document describing how the identified capabilities need to function from a cross-component perspective to support the Analysis of Alternatives for the Tunnel Detection and Technology Program
- Provide oversight to ensure that CBP identifies and considers key operational dependencies, relationships, and corresponding program risk for CBP's Tunnel Detection and Technology Program efforts prior to approving the program
- Designate an authority to provide leadership, strategy, and coordination of DHS countertunnel efforts

Detecting tunnels is currently a slow and labor-intensive process requiring higher technology, and is facing three major challenges (Shi 2009): (1) location of the tunnel, (2) depth and dimension of the tunnel, and (3) unfavorable subsurface geological/geophysical conditions. Detecting tunnels by conventional geophysical means with a subsurface sensor grid, even for very shallow targets, has been difficult due to the surface sensor's limited penetration and low profile of the tunnels (Shi 2009). Ground-penetrating radar (GPR) has the best potential to provide rapid and high-resolution images and to detect tunnels under favorable operating conditions (Shi 2009). However, the application potential of GPR over a vast majority of areas on the US border is very limited due to geological and geophysical conditions (Shi 2009).

Robert Ballard (1982), of the US Army Engineer Waterways Experiment Station (WES), pointed out that tunnel detection by aerial and satellite remote-sensing methods as proven to be relatively ineffective. Use of satellite photography, infrared imaging, and so on can be used to detect spoil areas; however, deep-based tunneling activity has thus far eluded state-of-the-art remote-sensing technology (Ballard 1982). While WES has not participated in a first-hand evaluation of remote-sensing methods, WES contacts with Mobility Equipment Research And Development Command (MERADCOM), the Engineering Topographic Laboratory, US Geological Survey, and other agencies involved in remote-sensing substantiate the fact that no clandestine tunneling activities have been remotely detected (Ballard 1982). Nearly all known methods proposed for detection are based on geophysical technology and have had either little or no consistent or reliable success as a result of various limitations (Geoconsol 2013).

8.10.1 Ground-Penetrating Radar

GPR does not work well in moist mediums like clay or below the water table, and rarely penetrates deeper than 12 m, and false alarms even at shallow depths are not uncommon (Geoconsol 2013).

8.10.2 Seismic Waves

Seismic waves require real-time detectors and more powerful imaging software to filter out the waves' reactions to natural and man-made noises, such as wind and highway traffic (Geoconsol 2013).

8.10.3 Electrical Resistivity

Electrical resistivity would require a wide-ranging network and would have to be permanently installed, at great expense, and it would have to be hidden to avoid tampering (Geoconsol 2013). Measurements would then be taken of the resistance between the probes (Allen et al. 2008). Variations in resistance readings are expected to be small locally, with larger differences appearing gradually over larger distances; therefore, where resistance values contrast highly, a subsurface anomaly (such as a tunnel) is likely (Allen et al. 2008). Resistivity techniques allow for sensing penetration to depths greater than 100 ft with reasonably high accuracy, and have been used in the past to locate groundwater, chemical spills, and large voids (Sharma 1997).

8.10.4 Microgravity and Gravity Surveying

Microgravity methods have been used for the detection of cavities in Europe since the 1960s (Ballard 1982). Gravity anomalies occur when lateral density contrasts are present in the subsurface (Ballard 1982). Measurements of the gravitational

field do vary slightly; however, these variations are in the amount of mass between the earth's center and surface (Allen et al. 2008). The amount of missing mass due to a tunnel is small compared to the overall mass of the earth, meaning variation in the gravitational field will also be small and equipment to measure the variations must be highly sensitive (Allen et al. 2008). Microgravity would require very high precision (Geoconsol 2013). The gravity differential for a smuggling tunnel can be as slight as 10 μgal, measured against the earth's field of 100 million μgal (Geoconsol 2013). The precision of this method, however, is directly inverse to the sensing depth, unless the size of the features (tunnels) is proportionally larger (Allen et al. 2008).

8.10.5 Cosmic Rays

Cosmic rays would require a large number of costly detectors, buried beneath the probable paths of illicit tunnels (small detectors find few muons and therefore have low resolutions [Geoconsol 2013]).

8.10.6 Cross-Well Radar

Tunnels present both military and homeland security threats (Farid et al. 2008). Moreover, the threat of international terrorism has transformed the effort to detect tunnels into a national security priority to neutralize the risks of assailants entering military fortifications, high security facilities, or other target buildings by burrowing under them (Farid et al. 2008). Mahren and List (1995) used three radio-frequency (RF) electromagnetic field procedures (surface to surface, borehole to surface, and borehole to borehole) to detect and localize a 1371.6 cm (45 ft) deep tunnel across the United States–Mexico border near Otay Mesa east of San Diego, California, and achieved an acceptable level of success. Cross-well radar has also been proven efficient to confirm the existence of a deep tunnel through crystalline rock in the southern part of the Demilitarized Zone in the Republic of Korea (Allen 1992). Based on the experimental studies of Farid et al. (2008), the proposed method for tunnel detection and deterrence using cross-well radar is a promising solution. However, it is not versatile enough for large areas, and more of a confirmation technique for suspicious areas, especially for long-term monitoring of perimeters of highly secured areas, but the technique is not versatile for wide-range investigations (Farid et al. 2008).

8.10.7 High-Resolution Seismic Methods

The detection and delineation of underground cavities from the surface by geophysical means is a desirable goal (Steeples and Miller 1988). Previous seismic research intended to detect cavities due to salt-solution mining (Cook 1965), lava-flow tunnels (Watkins et al. 1967), and abandoned subsurface coal mines (Fisher 1971;

Hasbrouck and Padget 1982) had been unsuccessful. Most researchers using seismic techniques for cavity detection cite three phenomena for evidence of a cavity: free oscillations or resonance of the cavity walls, anomalous amplitude attenuation, and delay of arrival times (Cook 1965; Watkins et al. 1967; Fisher 1971). Voids in granite are deceivingly difficult to detect with reflection seismology, so in order to determine the seismic parameters that are critical to cavity detection in hard rock areas, Steeples and Miller (1988) conducted experiments across the top of the Moffat railroad tunnel near Winter Park, Colorado; this tunnel is 19 ft in diameter, through solid granite (Steeples and Miller 1988). Likewise, detecting the water tunnel was the next goal in the continued development and fine-tuning of the reflection technique for imaging voids, and they suspected the dominance frequency of the recorded energy was not high enough to detect the smaller tunnel (Steeples and Miller 1988). Thus, seismic reflection and diffraction methods were successfully used to detect the Moffat railroad tunnel at depths of 65 and 260 ft, the Moffat water tunnel at a depth of 65 ft, and abandoned coal mines in Pittsburg and La Cgyne, Kansas, at a depth of about 30 ft (Steeples and Miller 1988). Properly designed and implemented seismic reflection profiles have proven successful in detecting the presence of voids in a variety of geologic settings (Steeples and Miller 1988).

8.10.8 Approach to the Tunnel Detection Agent-Based Model

Based on the research and study developed by Ugarte et al. (2011), the exploratory data analysis, analytical models, system engineering and analysis, and modeling and simulation have been used to gain insights into sensor modeling and simulation to gain further insights into sensor allocation, configuration, placement, and prioritization of sensor field emplacement along the southern US border. The goals of the research were (Ugarte et al. 2011) (1) to develop a preliminary design of a prototype tunnel detection system as an asset for allocation/trade-off analysts' vignette in an agent-based model (ABM) environment; (2) to develop a data-farming methodology that lends itself with ease of use to analysts; and (3) to identify and define appropriate system measures. During model development, the notional node and sensor probability detection factors were created that defined both the characteristics and performance capabilities of sensors and the tunneling activities performed by an operator (Ugarte and Garcia-Olalla 2011). At the end of the study, the outputs are highly multivariate, consisting of all sensor system positions, dispositions, and strengths, as well as the perception of tunnel location (Ugarte et al. 2011). The common operational picture (COP) comprised the adversary and/or CBP tunnel interdiction assets (Ugarte et al. 2011). The measures of effectiveness (MOEs) that may be derived from ABM include time, assets, and money allocation, and the challenges to the tunnel defeat area attributed to the vast lengths of the border, varied geologies that degrade persistent monitoring and geophysical resolution of subsurface anomalies, as well as the unknown quantity of existing tunnels (Ugarte et al. 2011).

8.10.9 Electromagnetic Induction

Electromagnetic (EM) induction technology is a relatively new ground-surveying technique capable of subsurface imaging which uses a transmitter coil/antenna to generate an EM field that propagates into the ground (Allen et al. 2008). Additionally, salt and moisture, which have conductivity significantly higher than that of average soil, accumulate at the bottom of tunnels, making it possible to detect tunnels with no metal (Stolarczyk et al. 2005). A typical EM unit is carried in hand or pulled on a trailer (Allen et al. 2008). EM units can sense to depths approaching 100 ft or focus on shallow targets (Stolarczyk et al. 2007).

8.10.10 Tunnel Detection Using Forward Scatter between Borehole Signal Sources

If considering a tunnel as simply a cylindrical scattering object, it is clear that much of the scattering (diffraction) phenomena, which we will find useful in detecting and characterizing a tunnel, are best observed in or near the forward scatter direction (namely, the diffraction shadow of the tunnel or forward scatter enhancement) (Vesecky et al. 1980). This approach uses spatial variations in the scattered signal (Vesecky et al. 1980). Further, a question which immediately arises is whether EM waves or seismic P-waves are distinctively superior in tunnel detection work, and it is clear from the previous results of the Vesecky et al. (1980) model that seismic P-waves suffer much less attenuation during propagation and produce more salient tunnel signature for a given borehole separation; therefore, instrumentation limitations are important in any overall system evaluation.

8.10.11 Fiber-Based Brillouin Optical Time Domain Reflectometry

Fiber-based Brillouin optical time domain reflectometry (BOTDR) is the natural candidate for performing sensing measurement (Klar and Linker 2009). The ability of BOTDR sensors to provide distributed measurements of temperature and strain over tens of kilometers has been demonstrated in several studies (Horiguchi et al. 1990; Smith et al. 1999; Ohno et al. 2001). Although the sensitivity and/or spatial resolution of the early systems were rather limited, systems with sensitivity of less than 5 με and spatial resolution of 1 m are currently commercially available (Klar and Linker 2009). This improvement in performance has led to the use of BOTDR devices in a number of applications that require distributed strain measurements (Zeng et al. 2002; Zou et al. 2006). In particular, BOTDR devices are being used in geotechnical engineering to monitor the effect of excavations on pipelines and foundation piles (Klar et al. 2006; Vorster et al. 2006; Mohamad et al. 2007). Although these studies deal with the effects of excavation of larger tunnels, for underground transportation and water systems, they clearly demonstrate the ability

of the fiber-based BOTDR sensors to detect soil strains (Klar and Linker 2009). The proposed detection system is based on wavelet decomposition of the BOTDR signal followed by a neutral network (Klar and Linker 2009). Further research stages, and in particular field validation tests, are still required before such a system could become fully operational (Klar and Linker 2009).

Currently, tunnel detection technology risks (Shi 2011) include the following: (1) GPR may be ineffective in many urban environments; (2) unfavorable geophysical/geological conditions may limit detection; and (3) depth/dimensions of tunnels are highly variable, with small footprint. For future plans in detecting illegal tunnels, the following are important to consider (Shi 2011):

- Continuing sensor system development: (1) refine and optimize sensor system design and configuration, (2) refine data-processing algorithm, and (3) research on border soil environment condition
- Field testing: work with the potential customers to identify a specific operational environment for the future deployment and testing of the prototypes
- Prepare for the new collaboration with different agencies and organizations

8.11 Approaches for the Detection of Land Mines and Improvised Explosive Devices by Other Experts

An IED is a type of unconventional explosive weapon that can take any form and be activated in a variety of ways. It can target soldiers and civilians alike (NATO 2013). In recent years, innovative technology and procedures have helped lessen the danger of roadside bombings that soldiers face each and every day (Sutton 2012). The military is rushing new equipment to Afghanistan to help troops detect and detonate IEDs (Sutton 2012). However, insurgents have upped the ante by planting IEDs in different places in record numbers, making explosive devices a top killer of US troops in Afghanistan (Sutton 2012). According to the North Atlantic Treaty Organization (NATO), IEDs are the deadliest weapon in the insurgents' arsenal, accounting for more than half of all NATO casualties in the 11-year war (Pena 2013). The attraction of IEDs to adversaries is clear (NATO 2011). They are cheap and easy to make, using materials and components, including fertilizer-based explosives (often referred to as home-made explosives [HME] and commercial detonators, readily available for legitimate purposes which are often mass-produced (NATO 2011). NATO introduced a counter improvised explosive devices (C-IED) action plan with two main focus areas: defeating the device itself and disrupting the network (NATO 2013). With defeating the device, various branches within NATO look at how to detect and neutralize IEDs, prepare and train soldiers for an IED environment, develop technology to prevent IED attacks, and protect soldiers and civilians (NATO 2013). C-IED is not just about stopping or neutralizing an

IED once it is already in place, but also about identifying and disrupting the networks that create and initiate IEDs (NATO 2013).

8.11.1 Weapons Technological Intelligence

The Joint Improvised Explosive Device Defeat Organization (JIEDDO) leads DoD actions to rapidly provide C-IED capabilities in support of the combatant commanders and to enable the defeat of the IED as a weapon of strategic influence (JIEDDO 2011): lethal and nonlethal actions and operations against networks conducted continuously and simultaneously at multiple levels (tactical, operational, and strategic) that (JIEDDO 2011) (1) capitalize on or create key vulnerabilities, (2) disrupt activities, and (3) eliminate the enemy's ability to function; detection, mitigation, and neutralization of IEDs once they have been emplaced through (JIEDDO 2011) (1) route clearance, (2) device neutralization, (3) explosive detection, (4) disposal of unexploded and captured ordnance, and (5) vehicle and personnel protection; actions and activities designed to enable *Attack the Network* and *Defeat the Device* through (JIEDDO 2011)

- Graduate-level Combat Training Center events
- C-IED training at home stations and centers of excellence
- Focused individual C-IED predeployment training
- Training in-theater to stay ahead of adaptive enemy

Weapons technological intelligence (WTI) is a category of intelligence and a process derived from the forensic and technical collection and exploitation of IEDs, associated components, improvised weapons, and other weapon systems (JIEDDO 2013). WTI produces four products (JIEDDO 2013):

1. *Force protection*, which informs the warfighter of emerging threats; informs science, technology, research, and development; validates threats for testing; and documents electronic, physical, or event signatures.
2. *Targeting*, which distributes knowledge; analyzes and predicts patterns; maps devices to a group or person; analyzes links and networks; and conducts all-source fusion.
3. *Sourcing*, which identifies states or transnational sponsorships; tracks component movement; identifies manufacturing processes; and identifies network leadership financing.
4. *Support to prosecution*, matches individuals with a place, device, event, paraphernalia and/or weapon and compiles a forensic examination of latent prints, DNA, tool marks, assemble patterns and trace evidence.

The Terrorist Explosive Device Analytical Center coordinates and manages assets as the unified effort to technically and forensically exploit all IEDs throughout

the jurisdiction of law enforcement, intelligence community, and the Defense Department (JIEDDO 2013).

8.11.2 Ultra-Wideband Microwave Technology

Desperate to stay one step ahead of the roadside bombers, US Department of Defense (DoD) experts are now experimenting with ultra-wideband (UWB) microwave radar, a leading-edge medical diagnostic technology developed to locate malignant tumors (AT 2013). Research into landmine detection using UWB radar took place in the United Kingdom during the Falklands conflict in the early 1980s and in the United States in the aftermath of the Gulf War a decade later (AT 2013). UWB microwave imaging uses the measurement of the transmission of microwave energy through an object to define its dielectric (insulating) properties (AT 2013). A recent declassified NATO report on research into hand-held, standoff vehicle-based and airborne detection systems outlined some of the current and future engineering challenges affecting IED detection, recognition, and identification using UWB microwaves (AT 2013).

8.11.3 Foot Patrols

The US military's counterinsurgency strategy has emphasized increased use of foot patrols as a way to hunt down insurgents without endangering civilians, and as a result, troops are in a better position to find and defuse IEDs (Brook 2011). Although they conduct offensive operations based on specific intelligence reports, the soldiers accomplish most of their counterinsurgency through daily, key leader engagement patrols (Freeburg 2009). The soldiers rotate, so each squad patrols every 3 days (Freeburg 2009). Patrols can extend as far as 7 km, and each soldier carries about 60 lb of equipment through orchards, fields, mountainous terrains, and waterways (April 2009). Soldiers pack enough gear and supplies to last 48 h, in case they are delayed by enemy contact (April 2009). If soldiers discover an IED while on patrol, they must wait at that location until an explosive ordnance disposal team, or a military bomb squad, arrives to safely destroy or disable the device (April 2009). In April, troops on foot discovered more than 200 bombs before they blew up, about double the number from April 2010 (Brook 2011). But so-called dismounted operations come with a risk: greater chance of harm to the troops (Brook 2011). A US military survey of soldiers and marines in 2010 found that half said they had been within 55 yards of an IED that exploded while on foot patrol (Brook 2011). In 2010, bombs wounded 3366 US troops and killed 268 (Brook 2011).

8.11.4 Lasers to Find Land Mines and IEDs

Today we rely on dogs to sniff out hidden explosives and the problem is you can't debrief a dog, so you can't identify the kind of explosive or even be sure that the animal is smelling explosives rather than packaging material (Miles et al. 2012).

And who wants to risk the lives of dogs and their handlers (Miles et al. 2012)? There are many different ways a laser can sample the air above a suspected bomb (Miles et al. 2012). It can induce fluorescence or Raman scattering (which, like fluorescence, produces a signal with a distinct spectroscopic signature in the visible, infrared, or ultraviolet regions for each kind of molecule in the air) (Miles et al. 2012). Or, if it's powerful enough, the laser can turn the air into a bright spark, so that its molecular constituents break apart and each element emits its characteristic spectrographic signature (Miles et al. 2012). Now, researchers have developed an advanced new bomb detection technique that uses lasers no more powerful than your typical presentation pointer to detect and identify bombs like IEDs from tens, if not hundreds, of feet away (Gonzalez 2011). The bomb-detecting laser technology has already been demonstrated to work from up to 40 ft away, though the researchers estimate that it should work from upwards of 100 yards (Gonzalez 2011).

8.11.5 Laser Drilling and Analyzing System

The project named Laser Techniques for the Detection of IEDs (LIED) tries to develop systems for mobile platforms that can penetrate unknown objects and analyze their content for explosives and other materials with the help of generated gas components (AT 2010). The focus of the researchers lies on a laser-based intelligent drill technique to prevent accidental explosion of the materials, in particular, primary explosives. Such a system also needs means to analyze the gas components generated by the laser drilling (AT 2010). The final goal is a laser drilling and analyzing system, which could also include the capability to detect CBRN agents and be placed on a remote-controlled platform (AT 2010). Even those projects will not be able to detect every IED or roadside bomb because one of the main advantages of IEDs is their flexibility in matters of shape or explosive materials (AT 2010).

8.11.6 Terahertz Quantum Cascade Lasers

According to Reddy (2009), quantum cascade lasers (QCLs) are a new class of semiconductor lasers that are unipolar and can work effectively in mid-infrared and terahertz spectral regions even at room temperature. QCLs are thus ideal light sources for probing the strong fundamental vibration-rotational absorption bands of most gaseous molecules in nature which have tell-tale spectral finger prints in these spectral regions (Reddy 2009). Combined with sensitive laser spectroscopic techniques like cavity ringdown spectroscopy (CRDS) and photoacoustic spectroscopy (PAS), QCLs provide ultrasensitive detection capability to meet the challenge of standoff detection of lower concentration of IEDs and other hazardous chemicals in the field environment (Reddy 2009). Because of its low interference and nonionizing characteristics, terahertz imaging is expected to be a powerful technique for safe, in vivo medical imaging, where the use of longer wavelengths allows a deeper penetration in the investigated material

(Reddy 2009). QCLs in the mid-infrared to far-infrared including the THz region are really going to play a pivotal role in the investigation of new science and revisiting of most viable technologies (Reddy 2009).

8.11.7 Dogs for IED Detectors

Clearing patrol routes from the front, handlers and dogs are the first line of defense against the enemy's IED threat (Lodder 2012). While dogs are often a challenge to manage, they're vital to each mission (Lodder 2012). Their presence and proficiency help riflemen focus on their mission instead of worrying about striking an IED (Lodder 2012).

8.11.8 Radio Signal

One of the most common methods used to detonate IEDs is to trigger them remotely using a radio signal (HR 2008). Various common electronic items such as remote controls for toys and garage doors, key fobs for automobiles, two-way radios, cordless telephones, and cell phones have been used to detonate IEDs (HR 2008). JIEDDO has allocated much of its Defeat the Device funding to the development and fielding of vehicle-mounted and man-portable jamming equipment that prevent the trigger signal from reaching the bomb, and, currently, JIEDDO has fielded over 37,000 jammers (HR 2008). As attackers change frequencies and methods of attack, jammers must also be changed and it's important to note that if a jammer is effective, US personnel may not know, and the IED is then left to injure or kill others (HR 2008).

8.11.9 Talon II Remote-Controlled Robot/Intelligent Robots

Talon II remote-controlled robot (HR 2008) has been developed to investigate possible IEDs.

8.11.10 Mine Clearing Line Charge

Mine clearing line charge (MCLC, currently known as MICLIC) has been created and utilized to detonate hidden land mines beneath the ground surface. It is usually made of booster, main charges, propellant, and igniter. The common explosive that is used is C4 (plastic explosive) or Cyclonite (RDX). It is applicable to fused mines but does not necessarily destroy all land mines and it is also destructive and hazardous to the environment. The technology was being used in the 1940s. Other countries have their own technology similar to MICLIC: India—*Bangalore Torpedo*, Britain—British Python, Italy—SB 33 mine, and Japan uses their own MICLIC technology.

According to the US White House (WH) (2013), the US administration is expanding and broadening its C-IED focus, and building upon existing policy and strategy, which establish and implement measures to discover, prevent, protect

against, respond to, recover from, and mitigate IED attacks and their consequences at home or abroad.

8.12 Countering Nuclear and Radiological Threats

The US approach to preventing nuclear proliferation and nuclear terrorism includes three key elements (DoD 2010):

1. We seek to bolster the nuclear nonproliferation regime and its centerpiece, the Nonproliferation Treaty (NPT), by reversing the nuclear ambitions of North Korea and Iran, by strengthening International Atomic Energy Agency safeguards and enforcing compliance with them, by impeding illicit nuclear trade, and by promoting the peaceful use of nuclear energy without increasing proliferation risks.
2. We are accelerating efforts to implement President Obama's initiative to secure all vulnerable nuclear materials worldwide in 4 years.
3. We are pursuing arms control efforts—including the New Strategic Arms Reduction Treaty (New START), ratification and entry into force of the Comprehensive Nuclear Test Ban Treaty, and negotiation of a verifiable Fissile Material Cutoff Treaty—as a means of strengthening our ability to mobilize broad international support for the measures needed to reinforce the nonproliferation regime and secure nuclear materials worldwide.

The Defense Science Board Task Force on Nuclear Deterrence Skills was chartered to asses all aspects of nuclear deterrence skills—military, federal, and contractor—and to recommend methods and strategies to maintain a right-sized, properly trained, and experienced work force to ensure the viability of the US nuclear deterrent through 2020 (DoD 2008).

8.13 Mother Nature and Intelligent-Improvised Explosive Devices to Defeat Low-Tech IEDs, Land Mines, Other Hidden Weapons, and the Enemy

Attacks from IEDs are one of the major causes of American soldiers and marines being killed in action and wounded in action (DOA-USMC 2007). According to NATO (NATO 2012), IEDs play an increasingly important role and will continue to be part of the operating environment for future NATO military operations. NATO introduced a C-IED action plan with two main focus areas: defeating the device itself and disrupting the network. In this era of high technology, thousands of troops have still died in Iraq and Afghanistan and the death toll will continue to rise in the future if no effective strategy is implemented to defeat low-tech IEDs.

Based on literature research, there are some technologies and solutions currently being implemented and developed by other experts as presented in Sections 8.11, 8.11.1 through 8.11.9 (e.g., robots and foot patrols with bomb-sniffing dogs). However, these technologies and operations required some of the soldiers to go out in the danger zone to implement these technologies and would still be exposed in danger. Every individual soldier and marine who will be exposed in a dangerous war zone should be considered for safety and protection. A new potential capability could defeat IEDs and land mines with the employment of *weather and environmental modifications* (also known as "*Mother Nature"* as *support to warfare*) *integrated with intelligent-improvised explosive devices (i-IEDs) and gadgets*. These intelligent devices shall be made of materials that will interact with Mother Nature, the hydrologic cycle, as well as the materials of IEDs and other weapons. They can be effectively used to defeat the enemy during conflicts, while soldiers will not necessarily need to be in the danger zone.

The key purpose and considerations of this potential innovative capability are as follows:

- To enhance the effectiveness of protection and defense against the enemies and their weapons and to minimize soldier casualties. It will be essentially used to protect defense infrastructures in the combat zone and minimize risk of terrorist attacks.
- To detect and defeat enemies.
- To have the ability to calculate the distances/ranges of the enemies' locations.
- To target their locations or hideouts without causing casualties to our soldiers and allies.
- To disrupt and detect IEDs, land mines, and weapons.
- To retain the survivability and security of US armed forces and allies.

The potential *intelligent improvised devices* can be designed and modified to support homeland and critical infrastructure protection as "defensive systems" for aboveground, underwater, and underground uses mentioned in the previous chapters. Engineering planning and design for the interoperability of other protective and defensive systems can be done with this capability.

8.14 Conclusion

Security and preventive measures are always considered by experts, stakeholders, and decision-makers to be implemented for the protection of homeland and critical infrastructures. However, enemies always come up with stronger forces to defeat the current security measures. Law enforcement, firefighters, and emergency response teams cannot always immediately deter terrorist enemies and self-radicalized individuals. The technological "defensive approaches" should also be

implemented in conjunction with other countermeasures for the protection of critical infrastructures and public safety. These intelligent technologies can be designed to detect and discriminate weapons and enemies and be capable of terminating the enemies before they can even generate public injury and destruction to infrastructures. Additionally, the development of *Mother Nature (another term for "weather and environmental modifications") to be utilized for warfare* integrated with i-IEDs and other intelligent technologies could be very efficient, cost-effective, and useful for detecting and deactivating land mines and IEDs. The i-IEDs will be made up of materials and chemical compounds that will have a capability to function with Mother Nature. Further, risk acceptability analysis based on the quantitative psychology of intuitive judgments can be utilized to screen alternatives of defensive systems and to determine suitable special features of the technologies in support to national security.

References

Allen, J. 1992. Integrated geophysical approach to the detection of buried objects and clandestine tunnels. *Proc. SPIE Int. Soc. Opt. Eng.*, 1693:161–169.

Allen, L., Birrell, M., Borowski, K., Korth, S., Obermeyer, S., and Tesla, E. 2008. Technologies for the detection and monitoring of clandestine underground tunnels, USSTRATCOM Global Innovation and Strategy Center (GISC). http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA497908 (accessed April 21, 2013).

American Gas Association (AGA). 2002. Natural gas distribution industry critical infrastructure security, Natural Gas Infrastructure Security—Frequently Asked Questions.

Army-Technology. 2010. Getting close to IEDs. http://www.armytechnology.com/features/feature89054 (accessed on April 21, 2013).

Army-Technology. 2013. Hidden agenda: IED detection using ultra-wideband radar. http://www.army-technology.com/features/featureied-detection-ultra-wideband-microwave-radar-darpa-jieddo (accessed April 21, 2013).

Ballard, R. 1982. Tunnel detection. US Army Engineer Waterways Experiment Station, Technical Report GL-82–9. https://doc-0k-58-docsviewer.googleusercontent.com/viewer/securedownload/tm9cini2jrjmcl6urcf9l43kb2srjmb3/l91k5r55ap3ov578m5164moor700v873/1366519500000/Ymw=/AGZ5hq-1QT7sEf5OzsAl_zdHH_Jm/QURHRUVTaDJOUzAtYTlvVDgzamtyWHRxSlpOcE5aYVNLdktJaGRadElwRGxnUXlWaUlKb2dlYnpFSm9reU1IRmVuVERQaTZoVmJnV1k0TkVyU3d0LW9ncFN6dk54czhIZzNuaVFONURrdGUzUHk1dXgwU1c1N1d5TWtJUF9OWURZSG9oZzZXRks1V2o=?docid=e0c8416648e4b571a814ac29677daac4&chan=EQAAAG77frrnZbh1vIhluf6Cw%2BfDbCtoeBI/PDSC8/cwcBQz&sec=AHSqidZfvTGMqoL_6xUVObEhTiQdYLkoraHTgqZxpO6pqu8aX4Uvk0adse-LiNT-HNIUTMjygUes&a=gp&filename=GetTRDoc&nonce=p9v4u7o4jvqma &user=AGZ5hq-1QT7sEf5OzsAl_zdHH_Jm &hash=kaa10319fd6vhqsm0d989u6vehddghfn (accessed April 21, 2013).

Brook, T. V. 2011. Foot patrols in Afghanistan boost IED detection. http://usatoday30.usatoday.com/news/military/2011–05–23-military-IED-Afghanistan_n.htm (accessed on April 21, 2011).

Cook, J. 1965. Seismic mapping of underground cavities using reflection amplitudes. *Geophysics* 30(4): 527–538.

Farid, A., Martinez-Lorenzo, J., Alshawabkeh, A., and Rappaport, C. 2008. Tunnel detection using cross-well radar. *GeoCongress* 2008:284–291. http://ascelibrary.org/doi/abs/10.1061/40972%28311%2936 (accessed on April 20, 2013).

Fisher, W. 1971. Detection of abandoned underground coal mines by geophysical methods: USEPA water pollution control research series. Project 14010EHN, Washington, DC, p. 94.

Freeburg, E. 2009. Infantry foot patrols disrupt insurgents, aid remote Afghan Villages. http://www.army.mil/article/25544/ (accessed on April 21, 2013).

Geoconsol. 2013. Technology: Covert tunnels. http://www.geoconsol.com/publications/Covert_Border_Tunnel_Detection.pdf (accessed April 20, 2013).

Gonzalez, R. 2011. New lasers can find bombs from 40-feet away. http://www.wired.com/dangerroom/2011/09/new-lasers-can-find-improvised-bombs-from-40-feet-away/ (accessed April 21, 2012).

Hasbrouck, W. and Padget, N. 1982. Use of shear wave seismics in evaluation of strippable coal resources. *Utah Geol. Miner. Surv. Bull*. 118:203–210.

Horiguchi, T., Kurashima, T., and Tateda, M. 1990. A technique to measure distributed strain in optical fibers. *IEEE Photonics Technol. Lett*. 2:352–354.

Joint Improvised Explosive Device Defeat Organization. 2011. Attacking the IED Network. http://www.dtic.mil/ndia/2011GlobalExplosive/Gaghan.pdf (accessed April 21, 2013).

Joint Improvised Explosive Device Defeat Organization. 2013. Weapons Technological Intelligence. https://www.jieddo.mil/attack.aspx (accessed April 21, 2013).

Klar, A. and Linker, R. 2009. Feasibility study of the automated detection and localizing of underground tunnel excavation using Brillouin optical time domain reflectometer. http://gwri-ic.technion.ac.il/pdf/gwri_abstracts/2009_1/16.pdf (accessed April 21, 2013).

Lodder, R. 2012. Dogs of war: Friends and Saviors of Marines in Afghanistan. http://marines.dodlive.mil/2012/04/05/dogs-of-war/ (accessed April 21, 2013).

Mahren, K. and List, D. 1995. Radio frequency electromagnetic tunnel detection and delineation at otay mesa site. *Geophysics* 60(2):413–422.

Miles, R., Dogariu, A., and Michael, J. 2012. Using lasers to find land mines and IEDs. http://spectrum.ieee.org/semiconductors/optoelectronics/using-lasers-to-find-land-mines-and-ieds (accessed April 21, 2013).

Mohamad, H., Bennett, P., Soga, K., Klar, A., and Pellow, A. 2007. Distributed optical fiber strain sensing in a secant piled wall, *Proceedings of the 7th International Symposium on Field Measurements in Geomechanics, ASCE Geotechnical Special Publication (GSP)*, Boston, MA, Vol. 175, p. 81.

North Atlantic Treaty Organization. 2011. Countering Improvised Explosive Devices. http://www.nato.int/cps/en/natolive/topics_72809.htm (accessed April 21, 2013).

North Atlantic Treaty Organization. 2012. Countering Improvised Explosive Devised (c-IEDs). http://www.nato.int/cps/en/natolive/topics_72809.htm (accessed May 26, 2012).

North Atlantic Treaty Organization. 2013. NATO Air and Space Power in Counter-IED Operations. http://www.japcc.de/fileadmin/user_upload/Reports/CIED_2/NATO_Air_and_Space_Power_in_Counter-IED_Operations._A_Primer-Second_Edition.pdf (accessed April 21, 2013).

Ohno, H., Naruse, H., and Shimada, A. 2001. Industrial application of the BOTDR optical fiber strain sensor. *Opt. Fiber Technol.* 7:45–64.

Pena, A. 2013. Afghans struggle with IED detection, removal. http://www.stripes.com/news/afghans-struggle-with-ied-detection-removal-1.216522 (accessed April 21, 2013).

Radvanovsky, R. and McDougall, A. 2010. *Critical Infrastructure-Homeland Security and Emergency Preparedness*, 2nd edn., Boca Raton, FL: CRC Press.

Reddy, M. 2009. Terahertz quantum cascade lasers for ultra-sensitive detection of explosives and improvised explosive devices. http://drdo.gov.in/drdo/pub/dss/2009/main/23-LASTEC.pdf (accessed April 21, 2013).

Roston, A. 2013. DHS ties to find tunnels below the surface. http://www.defensenews.com/article/20130313/C4ISR01/303130017/DHS-Tries-Find-Tunnels-Below-Surface (accessed April 21, 2013).

Ryan, K. 2002. Powerful protection. *Am. Gas* 84(4):23.

Sharma, P. 1997. *Environmental and Engineering Geophysics*, Cambridge, UK: Cambridge University Press.

Shi, W. 2009. Multi-sensor approach to the detection of clandestine tunnels. http://www.mitre.org/news/events/exchange09/1909M401.pdf (accessed April 21, 2013).

Shi, W. 2011. Innovative approach to the detection of cross-border clandestine tunnels. http://www.mitre.org/work/areas/research/2011iebriefings/43MSR002-AA.pdf (accessed April 21, 2013).

Smith, J., Brown, A., DeMerchant, M., and Bao, X. 1999. Simultaneous distributed strain and temperature measurement. *Appl. Opt.* 38:5372–5377.

Steeples, D. and Miller, R. 1988. Tunnel detection by high-resolution seismic methods. ftp://geom.geometrics.com/pub/seismic/Literature/S-TR68.pdf (accessed April 21, 2013).

Stolarczyk, L. and Peng, S. 2007. Advanced electromagnetic wave technologies for the detection of abandoned mine entries and delineation of barrier pillars. http://www.fhwa.dot.gov/engineering/geotech/hazards/mine/workshops/ktwkshp/ky0314.cfm (accessed April 21, 2013).

Stolarczyk, L., Troublefield, R., and Battis, J. 2005. Detection of underground tunnels with a synchronized electromagnetic wave gradiometer, stolar research corporation. http://www.dtic.mil/dtic/tr/fulltext/u2/a434554.pdf (accessed April 21, 2013).

Sutton, L. 2012. New IED Detection Equipment Sent to Troops in Afghanistan. http://www.nbcsandiego.com/news/local/Military-Sends-New-IED-Detection-Equipment-to-Afghanistan-180769091.html (accessed April 21, 2013).

Ugarte, M., Anderson, T., Langford, G., Nannini, C., McMurtine, T., Wolberg, S., and Brown, B. 2011. Team 13: US customs and border protection (CBP) analysis support: Tunnel detection system. http://harvest.nps.edu/scythe/issue8/team13-scythe8-idfw20-eversion.pdf (accessed April 21, 2013).

Ugarte, M. and Garcia-Olalla, O. 2011. Sensor emplacement network analysis for detection of cross border tunnels. http://neddimitrov.org/uploads/classes/201104NFG/student-projects/UgarteGarciaOlalla-USMexicoTunnels-ExecutiveSummary.pdf (accessed April 21, 2013).

US Army Combined Arm Center. 2010. Disaster response staff officer's handbook. http://usacac.army.mil/cac2/call/docs/11–07/app_g.asp (accessed November 15, 2010).

US Congressional Research Service. 2010. Federal evacuation policy: Issues for congress. Linsay, B. http://www.dtic.mil/cgibin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA520742 (accessed June, 20, 2010).

US Department of the Army–United States Marine Corps. 2007. Improvised Explosive Device Defeat (FMI 3-34.119/MCIP 3-17.01.) http://www.fas.org/irp/doddir/army/fmi3–34–119-excerpt.pdf (accessed May 1, 2012).

US Department of Defense. 2008. Nuclear deterrence skills. http://www.defense.gov/npr/docs/dsb%20nuclear%20deterrence%20skills%20chiles.pdf (accessed April 21, 2013).

US Department of Defense. 2010. Nuclear posture review report. http://www.defense.gov/npr/docs/2010%20nuclear%20posture%20review%20report.pdf (accessed April 21, 2013).

US Department of Homeland Security. 2008. Homeland Security Presidential Directive 5. http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm (accessed June 20, 2010).

US Department of Homeland Security. 2012. Office of inspector general: CBP's strategy to address illicit cross-border tunnels, OIG-12–132. http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_SLP_12-132_Sep12.pdf.

US Federal Emergency Management Agency. 2004. National incident management system. http://www.fema.gov/good_guidance/download/10243 (accessed October 26, 2010).

US Federal Emergency Management Agency. 2008a. Mobile national response framework. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (accessed October 1, 2010).

US Federal Emergency Management Agency. 2008b. The mass evacuation incident Annex. http://www.fema.gov/pdf/emergency/nrf/nrf_massevacuationincidentannex.pdf (accessed October 1, 2010).

US Federal Emergency Management Agency. 2013. National response framework. http://www.fema.gov/national-response-framework (accessed May 13, 2013).

US Government Accountability Office. 1991. Trans-Alaska pipeline: Ensuring pipeline's security. Washington, DC. GAO/RCED-92–58BR. https://www.hsdl.org/?view&did=291 (accessed January 3, 2013).

US Government Accountability Office. 2008. National response framework: FEMA needs policies and procedures to better integrate non-federal stakes-holders in the revision process. http://www.gao.gov/new.items/d08768.pdf (accessed October 25, 2010).

US House of Representatives. 2008. The joint improvised explosive device defeat organization: DOD's fight against IEDs today and tomorrow. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA490963&Location=U2&doc=GetTRDoc.pdf (accessed April 21, 2013).

US Office of the Director of National Intelligence. 2007. An overview of the United States intelligence community. http://www.dni.gov/who_what/061222_DNIHandbook_Final.pdf (accessed August 22, 2010).

US Office of the Under Secretary of Defense for Policy. 2010. Homeland Defense and America's Security Affairs: FAQ. http://policy.defense.gov/hdasa/faq.aspx (accessed August 23, 2010).

US White House. 2013. Countering improvised explosive devices. http://www.whitehouse.gov/sites/default/files/docs/cied_1.pdf (accessed April 20, 2013).

Vesecky, F., Nierenberg, W., and Despain, A. 1980. Tunnel detection. SRI International, Defense Advance Research Projects Agency. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB372/docs/Underground-1980Tunnel.pdf (accessed April 20, 2013).

Vorster, T., Soga, K., Mair, R., Bennett, P., Klar, A., and Choy, C. 2006. The use of fibre optic sensors to monitor pipeline response to tunneling. In Don J. DeGroot; Jason T. DeJong; David Frost; and Laurie G. Baise., *GeoCongress 2006: Geotechnical Engineering Information Technology Age*, ASCE, Atlanta, GA, pp. 1–6.

Watkins, J., Dodson, R., and Watson, K. 1967. Seismic detection of near-surface cavities, US Geological Survey, Professional Paper 599-A, p. 12.

Zeng, X., Bao, X., Bremner, C. Brown, A., DeMerchant, M., Ferrier, G., Kalamkarov, A., and Georgiades, A. 2002. Strain measurement in concrete beam by use of the Brillouin-scatering-based distributed fiber sensor with single-mode fibers embedded in glass fiber reinforced polymer rods and bonded to steel reinforcing bars. *Appl. Opt.* 41:5105–5114.

Zou, L., Bao, X., Ravet, F., and Chen, L. 2006. Distributed Brillouin fiber sensor for detecting pipeline buckling in an energy pipe under internal pressure. *Appl. Opt.* 45: 3372–3377.

Homeland Security

Risk Assessment and Security for Pipelines, Tunnels, and Underground Rail and Transit Operations details a quantitative risk assessment methodology for systematically analyzing various alternatives for protecting underground rail, oil and gas pipelines, pipeline freight transportation, and other tunnel systems from terrorism threats and other disasters. It examines the engineering, environmental, and economic impacts and addresses both direct and collateral damage.

The book emphasizes how to apply the methodology of quantitative psychology for effective risk assessment in homeland security, critical infrastructure, and defense—specifically, in protecting pipelines, tunnels, underground rapid rail, and transit systems.

- Outlines the background and system operations of pipelines, tunnels, underground rail, and transit systems as well as other super-speed futuristic trains
- Covers materials used for fabricating weapons of mass destruction and operations for terrorism
- Deals with the probabilistic risk estimation process, event tree analysis, and fault tree analysis
- Discusses the risk and vulnerability assessment tools and methodologies used by experts and governmental agencies

Approved for public release by the U.S. Federal Government, this book presents regulations, standard processes, and risk assessment models recommended by the U.S. Department of Homeland Security and other federal and state agencies. Describing how to evaluate terrorism threats and warnings, it details protocols for preventive measures and emergency preparedness plans that are based on economic analysis.

With comprehensive coverage that includes risk estimation and risk acceptability analysis, the book provides a foundational understanding of risk and the various defensive systems that can improve safety and security as well as thwart terrorists' efforts to sabotage critical infrastructure.

CRC Press
Taylor & Francis Group
an **informa** business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

K16433
ISBN: 978-1-4665-6932-4
90000
9 781466 569324

www.crcpress.com