

# **SECURING TRANSPORTATION SYSTEMS**

Edited by

**Simon Hakim • Gila Albert • Yoram Shiftan**



**WILEY**



## **SECURING TRANSPORTATION SYSTEMS**



# **SECURING TRANSPORTATION SYSTEMS**

---

Edited by

**SIMON HAKIM**

**GILA ALBERT**

**YORAM SHIFTAN**

This book is published under the auspices of the  
Center for Competitive Government,  
The Fox School of Business and Management,  
Temple University,  
Philadelphia, Pennsylvania.

**WILEY**

Copyright © 2016 by John Wiley & Sons, Inc. All rights reserved

Published by John Wiley & Sons, Inc., Hoboken, New Jersey  
Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at [www.copyright.com](http://www.copyright.com). Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Limit of Liability/Disclaimer of Warranty:** While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at [www.wiley.com](http://www.wiley.com).

*Library of Congress Cataloging-in-Publication Data*

Securing transportation systems / edited by, Simon Hakim, Gila Albert, Yoram Shiftan.

pages cm

Includes bibliographical references and index.

ISBN 978-1-118-97793-4 (cloth : alk. paper) 1. Transportation—Security measures.

2. Transportation—Safety measures. 3. Transportation—Effect of terrorism on.  
4. Terrorism—Prevention. 5. Freight and freightage—Security measures. I. Hakim, Simon, 1944—  
editor. II. Albert, Gila, 1965—editor. III. Shiftan, Yoram, editor.

HE194.S424 2015

363.28'7—dc23

2015007720

Cover image courtesy of iStockphoto © ultraforma

Set in 10/12pt Times by SPi Global, Pondicherry, India

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

1 2016

*This book is dedicated to our spouses: Ariel Albert,  
Galia Sharon-Hakim, and Alona Nitzan-Shiftan.*



# CONTENTS

<b>Contributors List</b>	<b>ix</b>
<b>Foreword</b>	<b>xiii</b>
<b>Preface</b>	<b>xv</b>
<b>1 Introduction</b>	<b>1</b>
<i>Gila Albert, Erwin A. Blackstone, Simon Hakim,     and Yoram Shiftan</i>	
<b>SECTION I MOTIVATION AND CHALLENGES</b>	<b>23</b>
<b>2 Terrorist Targeting of Public Transportation: Ideology and Tactics</b>	<b>25</b>
<i>Shmuel Bar</i>	
<b>3 On the Rationality and Optimality of Transportation Networks Defense: A Network Centrality Approach</b>	<b>35</b>
<i>Yaniv Altshuler, Rami Puzis, Yuval Elovici, Shlomo Bekhor, and Alex (Sandy) Pentland</i>	
<b>4 Adaptive Resilience and Critical Infrastructure Security: Emergent Challenges for Transportation and Cyberphysical Infrastructure</b>	<b>65</b>
<i>Corri Zoli and Laura J. Steinberg</i>	
<b>5 Travelers' Perceptions of Security for Long-Distance Travel: An Exploratory Italian Study</b>	<b>91</b>
<i>Eva Valeri, Amanda Stathopoulos, and Edoardo Marcucci</i>	
<b>6 Securing Transportation Systems from Radiological Threats</b>	<b>109</b>
<i>Eric P. Rubenstein, Gordon A. Drukier, and Peter Zimmerman</i>	

<b>7 Protecting Transportation Infrastructure against Radiological Threat</b>	<b>129</b>
<i>Ilan Yaar, Itzhak Halevy, Zvi Berenstein, and Avi Sharon</i>	
<b>SECTION II SECURITY CONSIDERATION FOR MODES OF TRANSPORTATION</b>	<b>149</b>
<b>8 Securing Public Transit Systems</b>	<b>151</b>
<i>Martin Wachs, Camille N.Y. Fink, Anastasia Loukaitou-Sideris, and Brian D. Taylor</i>	
<b>9 Railroad Infrastructure: Protecting an Increasingly Vulnerable Asset</b>	<b>177</b>
<i>Jeremy F. Plant and Richard R. Young</i>	
<b>10 Freight Railroad Security: A Case Study of Post-9/11 Effectiveness</b>	<b>189</b>
<i>Roland D. Pandolfi, Jr.</i>	
<b>11 Cost-Effective Airport Security Policy</b>	<b>205</b>
<i>Robert W. Poole, Jr.</i>	
<b>12 Seaport Operations and Security</b>	<b>233</b>
<i>Willard Price and Ali Hashemi</i>	
<b>13 Pathologies of Privatization in the Transportation Worker Identification Credential Program</b>	<b>257</b>
<i>Benjamin Inman and John C. Morris</i>	
<b>14 Traveler's Security Perceptions and Port Choices</b>	<b>271</b>
<i>Amalia Polydoropoulou and Athena Tsirimpa</i>	
<b>15 Pipeline Security</b>	<b>281</b>
<i>Luca Talarico, Kenneth Sørensen, Genserik Reniers, and Johan Springael</i>	
<b>SECTION III THE ROLE OF TRANSPORTATION IN EVACUATION</b>	<b>313</b>
<b>16 Evacuation from Disaster Zones: Lessons from Recent Disasters in Australia and Japan</b>	<b>315</b>
<i>Daniel Baldwin Hess and Christina M. Farrell</i>	
<b>17 Evacuation Planning and Preparedness in the Aftermath of Katrina, Rita, Irene, and Sandy: Lessons Learned</b>	<b>345</b>
<i>David S. Heller</i>	
<b>18 Rural Evacuation and Public Transportation</b>	<b>363</b>
<i>Jaydeep Chaudhari, Zhirui Ye, and Dhrumil Patel</i>	
<b>Index</b>	<b>377</b>

# **CONTRIBUTORS LIST**

**Gila Albert**, The Ran Naor Foundation for the Advancement of Road Safety Research, Hod Hasharon, Israel; and Faculty of Technology Management, HIT – Holon Institute of Technology, Holon, Israel.

**Yaniv Altshuler**, Media Lab, Massachusetts Institute of Technology, Cambridge, MA, USA.

**Shmuel Bar**, Samuel Neaman Institute for National Policy Studies, Technion Israel Institute of Technology, Haifa, Israel.

**Shlomo Bekhor**, Transportation Research Institute, Technion – Israel Institute of Technology, Haifa, Israel.

**Zvi Berenstein**, The Nuclear Research Center Negev (NRCN), Israel Atomic Energy Commission (IAEC), Negev, Tel Aviv, Israel.

**Erwin A. Blackstone**, Center for Competitive Government, Fox School of Business & Management, Temple University, Philadelphia, PA, USA.

**Jaydeep Chaudhari**, Western Transportation Institute, Montana State University, Bozeman, MT, USA.

**Gordon A. Drukier**, Image Insight, Inc., East Hartford, CT, USA.

**Yuval Elovici**, Department of Information Systems Engineering and Telekom Innovation Laboratories, Ben-Gurion University, Beer Sheva, Israel.

**Christina M. Farrell**, Regional Institute, University at Buffalo, State University of New York, Buffalo, NY, USA.

**Camille N.Y. Fink**, American Planning Association, Chicago, IL, USA.

**Itzhak Halevy**, The Nuclear Research Center Negev (NRCN), Israel Atomic Energy Commission (IAEC), Negev, Tel Aviv, Israel.

**Ali Hashemi**, Eberhardt School of Business, University of the Pacific, Stockton, CA, USA.

**Simon Hakim**, Center for Competitive Government, Fox School of Business & Management, Temple University, Philadelphia, PA, USA.

**David S. Heller**, Regional and Systems Planning, South Jersey Transportation Planning Organization, Vineland, NJ, USA.

**Daniel Baldwin Hess**, Department of Urban and Regional Planning, University at Buffalo, State University of New York, Buffalo, NY, USA.

**Benjamin Inman**, School of Public Service, Old Dominion University, Norfolk, VA, USA.

**Anastasia Loukaitou-Sideris**, Department of Urban Planning and Institute of Transportation Studies, Luskin School of Public Affairs, UCLA, Los Angeles, CA, USA.

**Edoardo Marcucci**, DISP, CREI, University of Roma Tre, Rome, Italy.

**John C. Morris**, School of Public Service, Old Dominion University, Norfolk, VA, USA.

**Roland D. Pandolfi, Jr.**, Union Institute & University, North Miami Beach, FL, USA.

**Dhrumil Patel**, College of Education and Human Sciences, University of North Alabama, Florence, AL, USA.

**Alex (Sandy) Pentland**, Media Lab, Massachusetts Institute of Technology, Cambridge, MA, USA.

**Jeremy F. Plant**, Department of Public Policy and Administration, Penn State Harrisburg—The Capital College, Pennsylvania State University, Middletown, PA, USA.

**Robert W. Poole, Jr.**, Reason Foundation, Los Angeles, CA and Washington, DC, USA.

**Amalia Polydoropoulou**, Department of Shipping Trade and Transport, University of the Aegean, Chios, Greece.

**Willard Price**, Eberhardt School of Business, University of the Pacific, Stockton, CA, USA.

**Rami Puzis**, Deutsche Telekom Lab, Department of Information Systems Engineering, Ben-Gurion University, Beer Sheva, Israel.

**Genserik Reniers**, Department of Engineering Management, Faculty of Applied Economics, University of Antwerp, Antwerp, Belgium; Safety Science Group, University of Technology Delft, Delft, The Netherlands; and Center for Corporate Sustainability (CEDON), HUB, KULeuven, Brussels, Belgium.

**Eric P. Rubenstein**, Image Insight, Inc., East Hartford, CT, USA.

**Amanda Stathopoulos**, McCormick School of Engineering & Applied Science, Northwestern University, Evanston, IL, USA.

**Avi Sharon**, The Nuclear Research Center Negev (NRCN), Israel Atomic Energy Commission (IAEC), Negev, Tel Aviv, Israel.

**Yoram Shiftan**, Transportation Research Institute, Technion – Israel Institute of Technology, Haifa, Israel.

**Kenneth Sørensen**, Department of Engineering Management, Faculty of Applied Economics, University of Antwerp, Antwerp, Belgium.

**Laura J. Steinberg**, College of Engineering and Computer Science, Syracuse University, Syracuse, NY, USA.

**Johan Springael**, Department of Engineering Management, Faculty of Applied Economics, University of Antwerp, Antwerp, Belgium.

**Luca Talarico**, Department of Engineering Management, Faculty of Applied Economics, University of Antwerp, Antwerp, Belgium.

**Brian D. Taylor**, Department of Urban Planning and Institute of Transportation Studies, Luskin School of Public Affairs, UCLA, Los Angeles, CA, USA.

**Athena Tsirimpa**, Transportation and Decision Making Laboratory, University of the Aegean, Chios, Greece.

**Eva Valeri**, European Commission, Joint Research Centre (JRC), Institute for Prospective Technological Studies (IPTS) Edificio Expo, c/Inca Garcilaso, Seville, Spain; and DEAMS, University of Trieste, Trieste, Italy.

**Martin Wachs**, Department of Urban Planning and Institute of Transportation Studies, Luskin School of Public Affairs, UCLA, Los Angeles, CA, USA.

**Ilan Yaar**, The Nuclear Research Center Negev (NRCN), Israel Atomic Energy Commission (IAEC), Negev, Tel Aviv, Israel.

**Zhirui Ye**, School of Transportation, Southeast University, Nanjing, China.

**Richard R. Young**, School of Business Administration, Penn State Harrisburg—The Capital College, Pennsylvania State University, Middletown, PA, USA.

**Peter Zimmerman**, King's College London, Arms Control Expert & Nuclear Physicist, London, UK.

**Corri Zoli**, Institute for National Security and Counterterrorism (INSCT), College of Law/Maxwell School of Citizenship & Public Affairs, Syracuse University, Syracuse, NY, USA.



# **FOREWORD**

The birth of the twenty-first century showed a rise in terrorist attacks by radical groups around the world which caused many in the West puzzled with the motives for attacks, the vulnerability of places, and type of infrastructure to such attacks and how to prepare in order to minimize damages. This book reviews the motives for terrorist attacks, the type and nature of attack that coincide with religious code, and how to efficiently and effectively prepare for an attack. Indeed, evidence suggests that airlines, interregional rail, subway, and terminals are especially vulnerable to attacks. The reason for terrorist attack on transportation systems is the expected mass number of casualties in mass gathering in an enclosed place and the media attention obtained to the event. Still vulnerability of transportation systems for disaster is quite low and thus allotment of public budget for protection and preparations is below suggestions of Congressional committees. Terrorists have the freedom to choose a target, the method of attack, and the timing while it is practically impossible to adequately protect vulnerable critical infrastructure. A standard protection can easily be overwhelmed by trained terrorists.

The book reviews attacks that have occurred against transportation systems and also reviews the suggested methods of preparation, and response and recovery from such disasters. The book touches upon an important incentive for greater involvement of the private and volunteer sectors in the process. Government production of service is often inefficient given its monopolistic stance and its nonprofit goal. Owners of Critical Infrastructure expect the government to provide these services and therefore limit their own efforts. Only 5% of the containers brought into the United States is checked for possible dirty bombs or biological or chemical agents that could spread harm or diseases. Shipping companies compare the cost of investing and operating security equipment while the blame for a possible disaster caused by

an infected container will not adversely affect their business. If haulers are held responsible for possible inclusion of hazardous material or are required to carry insurance policy, then they will spend more on developing detection devices. Accountability and non-reliance on government in providing homeland security services will unleash greater participation of the private sector in such efforts. Government could shed many of the security services they provide by auctioning them out to private and public entities. Creation of markets in the production of security could improve efficiency, innovations, and better services. By limiting government financial support to merely the public good portion will encourage owners of transportation infrastructure to innovate and improve efficient production. The time has come where government shift its responsibility from the production and financing security services to initiating and coordinating efforts, and generating information and strategies that are shared by government, businesses, and volunteers.

**Dean M. Moshe Porat**  
**Fox School of Business and Management,**  
**Temple University**

## **PREFACE**

Beginning in mid-2014, the world learned about ISIS, which aggressively joined other Islamic terrorist organizations and has been successful inspiring and recruiting many young Muslims from the United States and other Western nations. It is clear that the war will not remain just in Iraq and Syria, but the jihad will expand into terrorist activities in the Western world.

The main problem in defending against terrorism is inherent in its asymmetric nature. Terrorists can attack any specific target, at any place and time and with any means. Given limited budgets, this makes practically impossible effectively protecting against all such options. Also, terrorists have initiated new methods or attack, while homeland security efforts simply react to them by implementing specific defense. Airlines responded to smuggling weapons into aircrafts by implementing extensive body and luggage checks. Then, a terrorist tried to smuggle explosives in the soles of his shoes, which resulted in requiring all passengers to take off their shoes to be examined with other carry-on items. Unfortunately, it is difficult, if not impossible, for security forces to initiate effective measures before terrorists apply innovative attacks. Given the wide range of options available and the innovative methods that terrorist can apply, it is difficult for law enforcement agencies to effectively “harden” targets as is done against criminal activities. Law enforcement deterring activities are effective in lowering crimes but are ineffective in lowering terrorist activities. Without concrete intelligence or going on the offensive, it is impossible for law enforcement using “thin” efforts to effectively protect all possible targets. Clearly, a well-planned professional terrorist attack could usually overcome most such routine and “thin” protective measures.

The surprised attacks on the World Trade Centers, the Boston Marathon, and the Cercanías train system of Madrid, Spain, among others, showed that effective

budgeting should center more on response and recovery than on preventing activities. In general, the expected costs of an attack on any infrastructure equates to the probability of such an attack times the magnitude of the damages. The higher the expected costs, the greater should be the total amount allotted for its security. For a given total amount spent on securing a specific target, the allocation among prevention, response, and recovery activities could differ. The lower is the probability of an attack on a specific infrastructure, the greater the share to be spent on response and recovery activities. For, efficient budget allocation, the greater the probability of an attack, the more should be spent on preventive activities.

Terrorist attacks are aimed at causing large numbers of casualties with detrimental impacts in short as well as long run. Terrorists choose targets with low chance of their being identified and apprehended. Attacking transportation systems including major rail and airport terminals, subways, airlines, or passenger ships is attractive since the number of casualties can be large, and the consequent reduction in the use of these transportation systems often yields an economic slowdown. The September 11 attack caused over 3000 deaths and many injuries and led to a lengthy recession among airlines, hotels, tourist services, and many other related industries. These indirect adverse effects often last longer and are higher in magnitude than the direct damages.

It is quite easy for terrorists to carry concealed explosives or even a dirty bomb into a major rail or subway terminal. Technological means that “smell” nuclear, chemical, or biological emissions in crowded areas could help detect such attempts but unfortunately have not yet become practical. A cyberattack adds a new dimension to terrorism where an attack can be executed from a remote site by penetrating the computer network of the railroads, subways, or air controllers, causing disasters without endangering terrorist lives and with higher probability of success. Deploying massive law enforcement personnel at such infrastructures would be unlikely to prevent an attack but would entail a high cost. However, an effective regional response and recovery team that can be deployed to any site in the region, at any time, and deal with any situation and employ any method of response would probably be effective.

Public choice theory teaches us that political leaders will allocate few public funds toward activities of low probability of occurrence but involve high damages. On the other hand, for high probability of occurrence events with lower damages, more resources will be allocated even though the total expected costs for both may be the same. Elected government decision makers need public support and therefore prefer to support activities that induce short-term achievement. The same is true for private corporate executives that need to show profits in the short run and are less concerned with long-term consequences. Therefore, both public and private executives will spend less than desired on homeland security activities and are even less likely to devote sufficient funding to protecting against low probability attacks with high damages. Government intervention may be necessary to encourage such spending in order to protect both private and social interests.

Public administration theories on federalism suggest that the balance of power between the federal government and the 50 state governments is beneficial. When activities are shifted from the federal to state governments, there is greater chance

for innovations and entrepreneurial activities at the lower “less conventional” level than with the monopolistic federal government. Hurricanes Katrina and Rita in 2005 showed that the remote management of FEMA and the state government, both in distance and familiarity, contributed to ineffective response and recovery activities. Also, terrorist-initiated and natural disasters often affect several local and even state political jurisdictions. Thus, homeland security activities should be consolidated for all levels of government to a regional entity and become a public-private partnership.

This book suggests that because of self-interest of both public and for-profit executives, the budget for homeland security activities, including the protection of transportation infrastructure and activities, is likely to be below the socially desired level. Introduction of volunteers to the PPP can add flexibility, adaptive behavior, innovations, and more efficient resource allocation. To be successful, this team must control the budget, the “peacetime” political agencies and leader must relinquish their power to the team for all homeland security efforts, and if a disaster occurs, the team must control the entire affected area regardless of jurisdictional boundaries.

The premise of this proposed restructuring of homeland security management is that existing political leaders and other administrative executives in the public sector who currently manage homeland security services are usually trained and experience in “peacetime” activities and are less equipped for dealing with disasters. However, in most regions, there are former highly ranked military commanders or business executives who have the expertise and interest in leading, preparing, and managing unexpected and large-scale homeland security events. Usually, such leaders volunteer their services and are able to attract other executives to join the team. Volunteers who served the public in leadership capacities include former Mayor Michael Bloomberg of New York City who led the city for 12 years for \$1 a year salary. Other successful leaders are the late five-term US Senator Frank Lautenberg of New Jersey and Mitt Romney who saved the Winter Olympics and later was governor of Massachusetts. Such volunteers could contribute to effective preparation, response, and recovery and usually would do so without self-interest that could cause the allocation of resources to deviate from the social optima.

The editors of this book and the Center for Competitive Government of Temple University have studied the issue of securing critical infrastructure and are preparing detailed programs of implementing the above approach. Hopefully, such changes in preparation, response, and recovery from disasters could minimize possible consequences of future terrorist activities.



---

# 1

---

## INTRODUCTION

GILA ALBERT<sup>1,2</sup>, ERWIN A. BLACKSTONE<sup>3</sup>, SIMON HAKIM<sup>3</sup>,  
AND YORAM SHIFTAN<sup>4</sup>

<sup>1</sup>*The Ran Naor Foundation for the Advancement of Road Safety Research, Hod Hasharon, Israel*

<sup>2</sup>*Faculty of Technology Management, HIT – Holon Institute of Technology, Holon, Israel*

<sup>3</sup>*Center for Competitive Government, Fox School of Business & Management, Temple University, Philadelphia, PA, USA*

<sup>4</sup>*Transportation Research Institute, Technion – Israel Institute of Technology, Haifa, Israel*

### 1.1 OVERVIEW

Transportation systems are essential infrastructures for economic vitality, growth, and well-being throughout a country. These systems including airports, water ports, highways, tunnels and bridges, rail, and mass transit are inherently vulnerable to terrorist attacks, which dreadfully became an agonizing reality in the post-9/11 era. They might face various threats, namely, biological, chemical, nuclear (dirty bombs), cyber, and natural disaster. In fact, transportation systems continue to be a prime terrorist target (Carafano 2012).

Surface transportation is a soft target, offering terrorists relatively uncomplicated access and easily penetrable security measures. In addition, the large crowds at surface transportation facilities guarantee the attackers effectiveness and anonymity and facilitate their escape (Jenkins 2003; Potoglou et al. 2010). Therefore, terrorist attacks on various transportation systems are perceived an “efficient” means to hurt any civilization at its “soft belly.”

Transportation systems are also essential for evacuation when a natural disaster, a terrorist attack, or a man-made failure occurs. All types of emergency response

depend on the availability of functional roads and transportation assets (Edwards and Goodrich 2014). Efficient and effective evacuation can significantly mitigate the catastrophe consequences and therefore serves as one of the most promising means for response and recovery from such destructive incidents.

Terrorist attacks could lead to immediate and long-term catastrophic consequences. Terror, like other forms of disaster, could trigger adaptive behavior that reduces the risk of being involved in such a tragedy (Elias et al. 2013; Floyd et al. 2004; Kirschenbaum 2006). However, the changes in travel behavior may have broad and short- and long-term effects. In the short run, travelers may adopt new behavior, including changes in travel mode, routes, and destinations and even canceling some activities and postponing others (Elias et al. 2013; Exel and Rietveld 2001; Floyd et al. 2004; Holguin-Veras et al. 2003; Kirschenbaum 2006; Potoglou et al. 2010). Long-term effects may include a decrease in the market share of specific travel modes that are perceived as less secure (e.g., public bus transportation) and thereby may indirectly affect land-use patterns (Exel and Rietveld 2001; Holguin-Veras et al. 2003; Polzin 2002). Such changes can also impact ancillary industries dependent upon the affected modes of travel.

Security considerations may result in a multitude of changes in the planning, design, implementation, and operation of transportation systems (Holguin-Veras et al. 2003; Polzin 2002; Potoglou et al. 2010). In addition, they may affect financing and investments in transportation system security, which are an important tool available to decision- and policy makers in response to terrorist incidents (Polzin 2002; Sandler and Enders 2004). In this regard, the aviation security model and its security procedure in the post-9/11 era are not applicable to surface transportation, which cannot be protected in the way commercial aviation is protected. Trains and buses must remain readily accessible, convenient, and inexpensive (Jenkins 2001; Potoglou et al. 2010).

The objective of security procedures is to reach the level of security that will maximize net social benefits from the use of each transportation mode. It is recognized that various security procedures that relate to surface transportation may affect travelers' privacy and freedom (Potoglou et al. 2010). Therefore, transit agencies and security authorities have to consider the trade-off between security, mobility, and freedom and the expected negative effects of an attack. Policy-maker should evaluate the overall costs of security precautions, the decline in service, and the adverse privacy consequences in comparison to the expected damage of an attack. The latter may be evaluated by the cost of various potential attacks multiplied by their probability of occurrence. No doubt, planning for prevention, deterring, response, and recovery of transportation infrastructures as well as resource allocation and priority setting is a major consideration of professionals and decision makers.

This chapter provides a comprehensive assessment of timely and challenging issues in securing transportation systems against various types of terror attacks and deals with the role of transportation networks in evacuation. It presents "state-of-the-art" efforts to improve technological and managerial security during and after natural disasters and incorporates some insights from this book.

The chapter reviews recent terror incidents targeting transportation modes and infrastructure. It also incorporates research findings on terrorist motivation and response to terrorist attacks. Then, the chapter discusses the role of efficient transportation in large-scale evacuation. The following section presents potential solutions, mainly technological and managerial improvements of how to deter, prevent, and detect these attacks and recover from severe consequences. Then, we discuss the role of not-for-profit volunteers and the private sector in securing transportation systems. The chapter concludes with evaluation issues and policy implications.

## **1.2 MAJOR TERRORIST ATTACKS TARGETING TRANSPORTATION SYSTEMS**

Terror threats to transport systems and related infrastructure have become an agonizing reality. Before 9/11, isolated incidents all over the world may have appeared to be random: major terrorist attacks between the years 1920 and 2000 targeted surface transportation, mainly trains and buses, with bombing being the most common tactic (Jenkins 2003). This trend significantly increased after 9/11.

Lethal terror attacks on public transportation facilities occurred in the post-9/11 era in various countries. The March 2004 Madrid train bombing, the July 2005 London Underground and double-decker bus bombing, the July 2006 Mumbai train bombing, and the Moscow Metro bombing in March 2010 are all examples of the vulnerability of public transportation system and the catastrophic consequences of these attacks. At the end of 2013, three bomb attacks targeting mass transportation occurred in the city of Volgograd in southern Russia. In October 2013, suicide bombing took place on a bus; on December 29, 2013, at a railway station; and a day later, on a trolley bus. Overall, at least 40 innocent people were killed in these three attacks on Russian transportation.

Fortunately, some terrorist plots targeting subways and trains were averted: London in 2002 and 2003, Sydney in 2005, Milan in 2006, and Barcelona in 2008. New York City prevented two alleged terror attempts in recent years. In July 2006, the FBI announced that it had foiled a plot by foreign militants that was in its “talking phase” to detonate explosives in tunnels connecting New Jersey and Manhattan; and on May 1, 2010, a car bomb was discovered in Times Square. Indeed, New York’s subway system, which is uniquely attractive to terrorists, has repeatedly been the focus of briefings by counterterrorism agencies.

Israel’s surface transportation has continuously been a main target of terror attacks since the establishment of the state in 1948. In the period 1994–2006, 17 severe terror attacks occurred on Israeli public buses and such related infrastructures as bus stations, with each attack resulting in 10 or more fatalities and dozens of injuries (Butterworth et al. 2012; Johnston 2010). In Jerusalem, the capital of Israel, 117 citizens were killed in transportation-related terror attacks, and more than 770 were injured between 2001 and 2003. However, the Israeli experience especially during the Second Uprising (Intifada), which started in September 2000 and lasted through the end of 2006, enabled training drivers and employees in preventing disasters

and minimizing damages and caused changes in traveler behavior. Damages were also mitigated because the terrorists employed poor tactics and lacked professional bomb-making skills (Butterworth et al. 2012).

### 1.2.1 Terrorist Ideology and Tactics

Review of major terror attacks suggests that certain types of attacks are “preferred” by terrorists since they are considered “more fit” or “more legal.” Conventional wisdom asserts that terror acts stem from political, social, and economics causes. However, as Bar (2004) stated, it cannot be ignored that most devastating global terrorist attacks have been perpetrated in the name of Islam (Bar 2004). Moreover, as Bar further discusses in Chapter 2, the body of Islamic rulings relating to justification of modern mass killing of civilians serves as the guideline for many Islamic terror acts.

The Islamic terrorism takes into account its religious roots, the rulings of Islamic law (*shari’ah*), and the outline of Islamic legal experts (*fatwas*). The history of Islamic terrorism involved various tactics, while terrorists choose the course of action very carefully. Agonizingly somehow, the 9/11 terror attacks seem to indicate the end of the aircraft hijackings, most probably due to the rigorous and robust changes in security practices at airports.

The maritime terrorism threat, although low in volume, is a worrisome contingency due to its vast and largely global, unregulated, and opaque nature (Szylionwicz and Zamparini 2013). Between the years 1967 and 2007, only 0.9% of terrorist attacks in the United States involved maritime transport (Nowacki 2014) and in the past 15 years only 2% of all terrorist attacks around the world (Roell 2009). These attacks target both passenger vessels and containerized shipping (RAND Database of Worldwide Terrorism Incidents 2014) or “choke points” and mega harbors (Roell 2009). Several initiatives and regulations have been developed in the United States post-9/11 including “Automated Targeting System” (ATM), “Container Security Initiative” (CSI), and “Security and Accountability for Every Port Act” (SAFE) as described in Chapter 12 of this book by Price and Hashemi. Many initiatives have been adopted worldwide, such as the Proliferation Security Initiative (launched by the United States in 2003), a global effort to stop the trafficking of weapons of mass destruction that was endorsed by over 100 nations (Bureau of International Security and Nonproliferation 2014).

The suicide attacks targeting surface transportation, mainly trains, subways, and train stations, seem to be an increasing tactic in the post-9/11 era. The improved explosive devices used by terrorists lead to greater lethality (MIPT 2007; RAND Database of Worldwide Terrorism Incidents 2014). Shmuel Bar concludes in his chapter in this book that to combat the radical trend in Islam what may be necessary is a “Kulturkampf” of the orthodoxy against the radicals, but in the short run, the Western political and legal arsenal needs to adapt itself to the existence of a religious war.

Transportation, and especially surface transportation, need to be highly accessible and will remain a soft target for terrorists. These systems may face various additional threats, namely, biological, chemical, nuclear (dirty bombs), and cyber.

The main challenge is therefore to evaluate and develop a long-term strategy to cope with potential, rather than current, threats. In this regard, special consideration should be given to the threat of cyber.

### 1.2.2 Cyberterrorism

Cybersecurity, a concept that was first used by computer scientists in the early 1990s to underline a series of insecurities related to networked computers, has moved beyond to threats arising from digital technologies, innovations, and changing geopolitical conditions (Nissenbaum 2005; Nissenbaum and Hansen 2009).

Although terrorists still employ the traditional tactics, they may target information technology and networking by creating damages to their applications and respective infrastructures (Janczewski and Colarik 2008). Cyberterrorism can be defined as the intentional use of computer, networks, and the Internet to cause destruction and harm (Matusitz 2005). Terrorists can convey encrypted messages, recruit supporters, acquire targets, gather intelligence, camouflage activity, etc., with only limited risk to the attacker. This limited risk is a function of difficulties in distinguishing between a simple malfunction and an attack, in connecting an event with a result, in tracking the source of the attack, and in identifying the attacker; the widespread use of inexpensive, off-the-shelf technologies; and the vulnerability of computer systems (Tabansky 2011).

Information and communication technologies (ICT) are rapidly penetrating all modes of transportation. Cyberterrorism is a tool of destruction that may lead to various devastating effects on the transportation system. Cyberattacks can cause serious damage to a critical infrastructure, which may result in significant casualties. For example, an act of sabotage caused financial and other damages when 800,000l of untreated sewage were released into waterways in Maroochy Shire, Australia (Abrams and Weiss 2000).

Thus far, no incidents of cyberterrorism in the transportation system have been successful. However, in Haifa, the third largest metropolitan area in Israel, the Carmel Tunnels, a major road tunnel within the city, didn't function for several hours one day in September 2013. The common hypothesis is that the cause was a cyberattack that led to malfunctioning of the communication and control of the tunnel. In Chapter 15, Talarico et al. report that beginning in 2005 the number of documented cyberattacks against the computer-controlled pipeline systems has notably increased (a series of attacks in 2013 that targeted a gas compressor station, which is a key component in moving gas through pipeline networks in the United States). In Chapter 9, Plant and Young illustrate this threat to railroads. Commuter lines and regional railroads have computer-based signaling and communications systems, which are necessary for their operation and therefore are vulnerable to cyberattack. Moreover, as discussed by Pandolfi in Chapter 10, a sophisticated cyberattack against the computer platforms that operate the railroads is becoming more likely.

Zoli and Steinberg discuss in Chapter 4 emergent challenges for the transportation sector through adoptive notion of resilience as they apply to critical infrastructure security, including cyber control systems that are vulnerable to attacks and accidents.

As mentioned by Wachs et al. in Chapter 8, the subject matter of transit security is inherently dynamic, responding to the changing nature of threats and taking advantage of the availability of new technology. Cybersecurity, which was not a significant element of transit system operations just a decade ago, is widely viewed in 2015 as an important vulnerability that requires new forms of training as well as investments in new software and technology. As Zoli and Steinberg indicate, the 2013 US Department of Homeland Security (DHS) budget of \$60 billion includes a 74% increase in cyber expenditures, while the overall department funding has remained the same as in earlier years.

The cyber threat is asymmetric; no great investment is required to perpetrate cyberattacks. In contrast, defense against cyber threats must encompass all channels of attack and keep up to date with new developments. Cyberattacks are often a sophisticated combination of sabotage, espionage, and subversion (Rid 2012). Defense from cyberattack requires more resources and is becoming more difficult to control (Tabansky 2011).

### 1.3 THE ROLE OF TRANSPORTATION IN EVACUATION

Transportation systems are essential for evacuation when a terrorist attack, a natural disaster, or a man-made failure occurs. The bushfires in Victoria, Australia (2009); the nuclear accident in Fukushima, Japan (2011); the floods in the United Kingdom (2014); and the Hurricanes Katrina (2005), Rita (2005), Gustav (2008), Irene (2011), and Sandy (2012) in the United States showed the need for efficient large-scale evacuation methods. All types of emergency response depend on the availability of functional roads and transportation assets (Edwards and Goodrich 2014). There is no doubt that well-functioning, robust, and flexible managed transportation systems can significantly contribute to mitigate catastrophe consequences.

Large-scale evacuation utilizes existing transportation infrastructure, which requires early and continuous planning and training. In this regard, multimodal transportation networks for emergency evacuation scenarios are also in the forefront. For example, road tunnel evacuations have been studied through different evacuation models (Ronchi et al. 2012). Effective traffic management is also essential for efficient evacuation, for example, converting some roads to one way in the direction of evacuation.

Regardless of the cause or the type of disaster, various factors shape the procedure of evacuation. Among the most important are jurisdiction features (e.g., geographical area, population size, and density) and characteristics of the transportation systems (e.g., state of infrastructure, alternative modes of transport, and transport control). In evacuation, whether mandatory or voluntary, citizens with privately owned vehicles may evacuate in a timely manner, while public transportation-dependent residents remain behind. This is not always the case as when there is insufficient fuel supply in existing gas stations. In the case of public transit users, school bus systems, especially in rural areas, are ideal mode to evacuate people without a car. As Chaudhari et al. discuss in Chapter 18, school buses should be incorporated into a local emergency

management plan. Hess and Farrell in Chapter 16 suggest that oversight of emergency planning by national and state governments is justified; however, local officials are usually best positioned to manage disaster preparedness, response, and recovery efforts. Our proposal for improving disaster policy questions such belief.

Heller in Chapter 17 discusses lessons learned in the aftermath of Hurricanes Katrina, Rita, Irene, and Sandy. Effective emergency planning and response requires extensive interagency coordination and collaboration, involving a multitude of professional talents. While advances in technology and social media have provided emergency managers powerful tools to enhance emergency preparedness and response, it will take a continued collaborative effort between government, the private sector, and the public to ensure a truly resilient evacuation management system.

Furthermore, evacuation procedure will benefit from innovations in communication network, social media, and joint operation centers. As stated by Daniel Hess and Christina Farrell in Chapter 16, an effective emergency response system must have resilient methods of communication and consistent messaging, as communication is often the first system to fail in the chaos of an extreme event. Hess and Farrell emphasize the importance of clear messages and redundancy in communication systems, as disasters often cause accidental technological breakdowns due to infrastructure damage or intentional shutdowns as public security measures. To address these challenges, a disaster communication plan should possess multiple channels, including websites, social media, television, radio and print, and in the recent years, especially smartphones and emergency specialized apps.

#### **1.4 MARKET FAILURE LEADING TO A NEW MODEL OF PPP**

Hurricanes Katrina and Rita showed how government at the federal, state, and local levels failed to provide adequate services to the impacted areas (US Senate 2006: Executive Summary). Mobile telecommunications trailers and the staff to operate them were offered by a private company within few hours from the start of the flood. Buses were needed to evacuate people from the disaster neighborhoods, while available school buses were unused and left on flooded parking areas to be later disabled by the flood. The State of Louisiana requested desperately needed forklifts from out of state even though they were available from local businesses. Home Depot, Walmart, and other retailers had supplies necessary to protect residents and businesses from the flood delivered from other locations (Boaz 2005). The supplies were ready for sale at the impacted areas well before the hurricane arrived. Evacuees at the gathering places lacked adequate food and essential supplies, while truckloads of major suppliers were stopped along the way. Indeed, delivery was suspended or delayed by local law enforcement officers even for trucks just outside the stadium (Business Executives for National Security (BENS) 2006; Lieberman 2005; Theroux 2005). Some “learning by doing” was evident in the response and recovery efforts to Hurricane Sandy in October 2012. However, it is likely that businesses in a competitive environment are more adaptive to such occurrences than is monopolistic government.

Another problem in responding to disasters emanates from what is termed “peak time demand” for local police, fire, and ambulance services. Specifically, greater staffing is needed during disasters than in normal “nonpeak” periods. Moreover, a severe shortage in first responders to Katrina resulted, since some workers chose to help their families and did not report for their duties (US Senate 2006: 12).

The outcry that followed Hurricanes Katrina and Rita prompted federal, state, and local governments to improve delivery of response services. The accumulated “learning by doing” and diffusion of information made governments improve first response services to Hurricane Sandy in October 2012. However, we did not experience any structural changes that assure “built-in” incentives for improved services when disaster occurs. Five major reasons prevent socially optimal allocation of resources for homeland security services.

First, government’s monopolistic position in the delivery of emergency services impedes efficient homeland security services. Government often produces a given level of services at higher cost than could be produced under more competitive conditions. This phenomenon is not peculiar to government. Monopoly or noncompetition even in the private sector often leads to costs being higher than they should be or what economists call x-inefficiency (Shepherd and Shepherd 2004). Prior to their becoming more competitive, the automobile and airline industries had such a problem. Government often allocates resources to various services arbitrarily, which does not necessarily address societal preferences (Homeland Security News Wire 2011).

Second, existence of “peak time demand” for emergency personnel and equipment that is significantly greater than what government possesses for regular activities suggests that supply should closely follow the demand trends. Energy consumption is high in Northeast America during the winter peak of January–February and again in the height of the summer in July–August. These peak time demands are generally consistent over the years, and therefore electric companies can accommodate them by increasing capacity to satisfy peak time demand, by purchasing electricity from electric companies in other regions or by differentiated cost-based prices to avoid expensive investment in power plants. A similar problem exists for homeland security. However, unlike the electric power case, both the probability of occurrence and the costs of homeland security are uncertain.

A third factor that prevents a “built-in” improvement in government provision of emergency services is the rigid territorial boundaries of localities and states that dictate the availability of personnel and equipment. When a disaster occurs, local first responders are the first to respond. The state government later provides additional support with the National Guard and necessary supplies. When the president declares an area has suffered a disaster, FEMA then provides major assistance. It is important to note that all federal resources are channeled through the state and are not provided directly to the affected community. In most disasters, the local mayor is in charge of response and recovery activities. However, most events and their required response and recovery services are not confined to the legal boundaries of a locality, but become instead a regional disaster with similar necessary response and recovery efforts. Mayors and their subordinates usually have the experience and the knowledge for providing regular services and are less knowledgeable in dealing with emergency

events. The National Weather Service predicted that a major storm would batter New Orleans on Friday, 3 days before it did, and will topple the levees in New Orleans. The mayor did not order a mandatory evacuation until the following Sunday, a day before the storm hit the city (Moynihan 2009).

The rigidity of government boundaries and bureaucratic structure that may accommodate “peace time” events is likely not to suit emergency conditions. A homeland security occurrence may cross counties and state boundaries, requiring coordinated and even unified response and recovery efforts, which would probably be more efficient and achieve better results.

A fourth reason why households, businesses, and government devote too few resources to homeland security is its perceived low probability of occurrence and high cost. Households and businesses are ready to spend more on high probability of occurrence events with lower costs than on a homeland security event where the expected costs are the same. Households purchase homeowners insurance, compensating mostly when a burglary occurs—an event that has a high probability of occurrence but low costs. At the same time, households are reluctant to purchase flood insurance with low probability but higher costs even though the expected costs are probably higher for floods. Indeed, even with federally subsidized flood insurance premiums, 50% drop their coverage after 3–4 years (Michael-Kayan and Kunreuther 2012). Moreover, homeowners are typically unwilling to spend mitigation measures to reduce damages from flood or other disasters. For example, in earthquake prone areas of California a 1989 survey reported that only 5–9% of respondents adopted any damage mitigation measures (Kunreuther et al. 2013).

Businesses behavior is similar, since its executives are judged by the immediate annual or even quarterly profits; a natural or man-made disaster is likely to be faced by the future managers of the firm. Corporate managers thus have been criticized for being obsessively concerned with the short-run instead of long-run interest of the firm (Blodget 2012). They arguably reduce capital investment and other long-run projects.

Government behaves similar to the firm. Elected officials serve for a stipulated period of time and need to show their short-term achievements. Spending on homeland security is likely to benefit future officials, and therefore, current budget under-spending is likely to occur. Underfunding of pensions by government (and by business firms) illustrates the focus on immediate concerns. Thus, both business and governments underfund homeland security efforts. Noteworthy, exposure to competition will not bring the actual allocation closer to its socially desired level. However, public exposure to the threat to homeland security can increase efficiency. In general, citizens should be educated about the importance of taking the long-run view. It is appropriate for households, business leaders, and government officials to take the long-term view. Achieving the socially desired spending should be addressed by the provision of appropriate incentives. Such remedies are appropriate for all cases where the probability of an event is low, while the cost is very high. In the business world, stock and stock options for the managers that can be redeemed only after several years have become an important part of their compensation, promoting a longer-run view. An efficient mandatory insurance requirement could also help insure the

adoption of appropriate security precautions. Lower premiums would be attained by adopting the appropriate mix of security.

A fifth reason for government's ineffective response to disasters is the desire by officials to avoid mistakes. This is the familiar type 1 and type 2 errors where type 1 involves an action that is clearly wrong and type 2 involves a decision to delay that impose costs but is less clearly wrong (Sobel and Leeson 2006). In the case of disasters, this means taking actions prematurely could be clearly shown to be a mistake so the cautious behavior approach is to wait until the disaster is imminent. Profit-motivated businesses would be expected to take the more socially appropriate action as they evidently did in the case of Katrina (Sobel and Leeson 2006).

BENS, which is an interesting solution for this problem, started following 9/11 where business and government join forces in preparing and responding to disasters. This program promotes private participation in sharing security information and joining the state's emergency operations center. It created, among other things, a registry for business resources available in a disaster and a sharing of secured communication channels. New Jersey, Georgia, Missouri and Kansas, Southern California, Iowa, and Massachusetts have all established such partnerships.

Contracting out addresses the problem of inefficiency of monopolistic government. Business monopolies are often concerned with losing their dominance through entry to their markets of close substitute producers. Therefore, monopolistic firms often charge lower than short-run profit maximizing prices to prevent such entries. Government does not face such threat and thus could retain inefficient production and pay higher than competitive wages. Contracting out the services requires clear and quantitative definition of outputs. The more vendors compete, the greater efficiency in production and the closer the price is to marginal and average cost. However, as mentioned earlier, greater competition has no bearing on the other factors.

Contracting out services that leads to competition does not address the "peak time demand" issue. Local governments then need, usually without much advance notice, labor, equipment, specific expertise, and material resources that are beyond their regular capacity. Clearly, such resources must be planned for before disasters occur. Exposure to markets to satisfy peak time demand can only partially make the missing resources available. The electric company's alternative solutions of building power plants with excess capacity, buying power from other companies, or using price differentiation are irrelevant here. We propose for consideration a homeland security model that relies on the management and entrepreneurship of volunteers or what is commonly referred to as the third sector.

Many successful leaders who have completed their business or military careers are interested in contributing their talent to the public sector, sometimes as a precursor for a political career. Such leaders are often financially secure, have high integrity, and a proven record of building an enterprise or managing an organization. Examples include Michael Bloomberg who initiated and managed a huge telecommunication company. Then, for a dollar a year, he served for 12 years as mayor of the city of New York. He contributed to the city both his talent and equipment from his companies. The late Senator Frank Lautenberg pioneered in

building ADP, a firm that managed wage payments for large companies. He was elected five times to the US Senate and initiated many successful socially oriented campaigns. Mitt Romney was a successful business consultant and later was a successful head of Bain Capital. He is widely acclaimed for saving the winter Olympics at Salt Lake City and later turn to public service as the governor of Massachusetts and as a candidate for the presidency. There are numerous examples of generals who managed large military or subsequently other organizations who later devoted their efforts to public service. Business and military leaders who succeeded in their careers are likely to succeed and benefit the public. They are likely to perform at least as well as government civil servants who often lack business and entrepreneurship skills and experience. On occasion, such leaders volunteer for public service as a stepping stone toward an elected position. Involvement of such leaders in regional homeland security positions may provide new ideas and methods to existing public bureaucracy.

When a renowned business or military leader heads a regional homeland security voluntary entity, it will attract other midlevel managers to join in order to enhance relationships with other leaders and become members of such an “elite club.” It is likely that most regions include such leaders as residents. We propose that all homeland security issues including transportation infrastructure and services within a region will be under the control of this leader. We recognize the inherent difficulties and challenges of implementing such a proposal but recommended consideration as a potential vehicle to enhance homeland security.

As we suggested earlier, when a disaster occurs, localities face significant shortages in semiskilled workers including, among others, law enforcement officers, firefighters, and heavy equipment operators (Blackstone and Hakim 2013). Such usually low-paid workers cannot and should not be expected to volunteer their services. Nationwide, there are more than three times the number of private security officers than the combined federal, state, and local law enforcement agents (Blackstone and Hakim 2013). These private security officers are trained for their jobs and are usually registered with the state. Again, as in the case of equipment, most commercial establishments are closed during disasters and these officers are not being paid. It is possible to train and register those who want to be of such service during disasters. When an emergency occurs, private guards could be deputized to fulfill temporary duties of law enforcement agents.

Volunteers can be used for semiskilled tasks. Volunteers can be signed up at colleges and universities, churches and fraternal organizations, retirees, and emergency response groups. It is essential that volunteers register long before a disaster occurs, their background checks are performed, and specific training conducted. Usually, one-third of volunteers are assigned for medical tasks. Volunteers should be engaged periodically and not merely when a disaster occurs. The state usually provides localities with volunteers. Thus, registration should be made on the state’s website. Two such effective registry programs are the California Disaster Volunteer Network and the Washington State Emergency Registry of Volunteers. Volunteers that show up spontaneously at a disaster site without prior registry and training usually cause complications. The site for these volunteers should be away from the disaster area. Some

can still be used in a planned fashion for certain jobs like filling sandbags and cleaning rubble (Steen 2014).

When disaster occurs, there is excessive demand for buses, trailers, lift trucks, and other heavy equipment that is beyond the available equipment of municipal and county governments. At times of disaster, similar equipment in the private sector may be idle. Registry of all public and private equipment should be prepared along with clear delivery options, leasing agreements, and payments.

The leading volunteer team relies on a PPP council that aids and advises the leading team. This council includes the mayors and the directors of emergency services of the region's cities and executives of major regional businesses and transportation companies. The council may change depending on the level and geographical spread of the disaster.

The success of establishing a new organization for homeland security depends on few factors. First, it should not be an addition to existing public entities but rather should replace them. It is especially true when existing entities are part of different hierarchical jurisdiction, like local governments, while the new entity is a regional entity. Second, public budgets for homeland security should be directed to the newly created regional entity. The regional entity will be responsible for the allocation of homeland security appropriations within their jurisdiction. Third, the state should provide a legal foundation to the regional entity so that it could sign contracts with public, private, and volunteer organizations. Fourth, when a disaster condition is announced, all powers and responsibilities are shifted from the various government agencies involved in first response and related services to the regional entity. Fifth, this new entity is not constrained by government rules and regulations. It is created as an entity that behaves like a business with flexibility in all activities. Again, we do not address the difficulties or legalities involved in creating such an organization but simply propose it as a vehicle to stimulate thought and discussion about this important issue.

The discussion so far shows that both the business sector and personal short-run preferences could prevent attaining a long-run solution, which may be preferred. For example, a long-run solution where the business spends more on R&D may lead to greater discounted present value of profits. Thus, even in a market environment, businesses do not necessarily allocate resources in a manner that maximizes long-term profits. The same inefficiency exists for government resource allocation aimed to maximize societal welfare. Elected and top government officials focus on short-term rather than long-term achievement. Local governments, for example, are likely to underfund homeland security programs. On the other hand, volunteer organizations and personnel usually take the long-run view. Volunteers are likely to stay active in their positions for long periods because of both lack of a hierarchical structure and the “spirit of the job.”<sup>1</sup> However, use of volunteers could improve the societal use of resources.

This book deals with the security of transportation systems. All modes of transportation incorporate their own security forces whether part of the organization itself

<sup>1</sup>A good example is the long-term service of local volunteer firemen, and auxiliary policemen.

or contracted out to private security companies. Over 80% of all infrastructures in the United States are privately owned. This is also true for most of our rail system, water ports, and bus services. Regular security services should remain under the jurisdiction of their owners or operators. In a disaster, all responsibilities within the region are transferred to the regional entity. Representatives of these transportation systems should be part of the council. Transportation systems, unlike most other infrastructures, possess the following significant attributes:

- Bus, rail terminals, and airports generally include masses of people. Since the terrorists' goal is to inflict a major impact, such infrastructures clearly become prime targets.
- Immediate first response is to evacuate people from affected areas. Attacking or disabling major evacuation systems would yield additional loss of life, human suffering, and economic damages.
- Operating transportation systems are essential for recovery efforts and the longer-term economic and social return to normal state. Thus, targeting transportation facilities prolongs recovery. The 9/11 attack led to a significant decline in air travel, tourism, and an economic slowdown of many direct and indirect industries. The decline in GDP is estimated to have lasted a full 2 years (Jackson 2008).
- Terrorist access to major public transportation targets is relatively easy in comparison to power, water, and other infrastructures. Transportation systems are usually accessible, while access to other critical infrastructure is limited and can be easier guarded. Current technologies are still limited in detecting explosives or individuals who might approach critical points in targeted areas to inflict maximum damage.
- Maritime commerce involves hundreds of thousands of containers a year. Many of these containers move through several water ports before reaching a US harbor. Existing technology does not allow thorough checking of these containers even though an undetected dirty bomb poses a high threat. These containers are often immediately transferred to trucks for transit to various US destinations where the explosion may occur.

Government on its own cannot secure transportation facilities and cannot allocate sufficient resources for such efforts. Also, 85% of infrastructures are owned by private companies that are responsible for their own security. Government can initiate, cultivate, and encourage such efforts by providing appropriate incentives for the creation of the three sectors' joint regional homeland security authority.

## 1.5 SECURITY STRATEGY

Homeland security obligations are categorized into preparation, response, and recovery from terrorist or natural disasters. Preparation is the planning and building of effective force for the two tasks of response and recovery. Preparation involves all

activities prior to a disaster including management, deterrence, and prevention. Responses are the activities conducted immediately during the disaster and its immediate aftermath where the main goal is to save lives. Recovery activities extend over the long term and are intended to yield a quick return to normalcy. Our model in the previous section suggests that the authority is responsible for all three tasks with a major role in the preparation phase. The authority controls and coordinates all involved entities.

The authority is in charge of resource allocation to all three tasks and among all involved entities. In most regional jurisdictions, like metropolitan areas, several critical infrastructures could be subjected to terrorist attacks. Examples include airports, water ports, power stations, railway stations, bus terminals, and schools.

The objective is to allocate the available resources to the three tasks of preparation, response, and recovery in a manner that minimizes the expected value of all damages.

In preparation, the main expense is on deterring and preventing an attack. Deterring activities are indication that the place is well protected and the probability of a successful attack is low. Prevention activities are physical measures that make entry difficult, time consuming, and increase the probability of apprehension. In protecting structures from burglary, these activities entail relatively high probability for avoiding an actual burglary. However, deterrence is minimal for terrorists who target an infrastructure, and “conventional” preventive measures are easily overcome. Routine prevention measures are unlikely to prevent entry by well-trained terrorists. For example, an armed guard and a high fence are unlikely to deter or prevent terrorists who intend to capture children. Even routine security of a power station is unlikely to deter terrorists who intend to detonate an explosive. Professional terrorists can chose a region in which to attack, the target, the time, and the method, among many possible targets. At the same time, in the absence of precise intelligence, the “legal” community has limited information and budget to protect all potential targets against professional terrorists in any given region. Great asymmetry exists between the terrorists that initiate an attack and the “legal” community that protects against it. A “thin” level of protection of all potential targets will not deter and will provide insignificant protection against professional terrorists. The same principle holds in protecting against a major natural disaster. Thus, most public resources should be spent on effective mobile response units that could be dispatched to any location in the region.

Further, with existing data-mining activities and electronic surveillance, a major land attack on a critical infrastructure is almost impossible. A cyberattack that is prepared and executed from a distance requires significantly fewer financial resources and is likely to inflict greater damage without endangering terrorist lives. Even highly sophisticated cybersecurity could be ineffective for a few high-impact attacks. Thus, resources are better spent on response, preventing aftermath damages, and recovery efforts than on deterrence and physical preventive measures.

At the same time, some deterring and preventive measures are effective against less professional, self-motivated terrorists or people with emotional disturbances. Such minimal efforts are the responsibility of the infrastructure’s owners. Government’s role

is to encourage owners and managers of critical infrastructures to protect their facilities by linking damages to self-inflicted costs. A basic level of protection against an attack of nonprofessional terrorists is an integral part of “reasonable” protection by the owners of the facility. The incentive for such self-funded security arises from the prospect of liability suits against the property by third-party victims of an attack. The courts usually find commercial owners liable in law suits for damages when “reasonable” protection is lacking. It is reasonable to assume that these practices of the courts lead commercial and industrial establishments to undertake the minimum required level of protection.

## 1.6 BOOK STRUCTURE AND CHAPTERS

This handbook focuses on how to protect our transportation systems and how to better plan evacuation when severe disasters occur. It contains insights and recommendations from a group of internationally recognized experts and provides guidelines for policy and public decision making as well as suggestions for IT companies for possible new products. The following issues are addressed in the book:

- Technological measures and innovative solutions to target protection and response provisions to protect our transportation infrastructure, consider their feasibility, and provide an economic evaluation
- Institutional restructuring that may increase security for critical infrastructure, for example, public–private partnerships
- Changes in travel behavior as a response to terrorism and natural disaster
- Policy implication and recommendations for preparation, response, and system recovery

The book consists of 17 invited original chapters, which are categorized into three sections.

### 1.6.1 Section 1: Motivation and Challenges

This section includes six chapters explaining the motivation for terrorist attacks against transportation modes and infrastructure and derived challenges. It describes radiological, cyber, and nuclear threats; demonstrates the impact of fear of attack on the general public; and presents prevention as well as recovery challenges.

This section starts with Chapter 2 by Bar that describes the nature of Islamic ideology, the tactics, and the justification for attacking mass transportation. This leads to the conclusion that the tactical appeal for terrorists will not vanish, and therefore, the main challenge is how best to protect mass transportation from attacks or more likely to mitigate their damages.

In Chapter 3, Altshuler et al. consider efficient deployment schemes of surveillances and monitoring units in key locations of the network for homeland security

purpose. Zoli and Steinberg explore in Chapter 4 emergent challenges for the transportation sector through adaptive notions of resilience as they apply to critical infrastructure security. In Chapter 5, Valeri et al. analyze the impact of security on long-distance travel behavior and investigate changes in travel and mode choices in response to variations in security levels and features. In Chapter 6, Rubenstein et al. review radiological and nuclear weapon threats to transportation systems and discuss methods to mitigate them. The first section ends with Yaar et al. who describe in Chapter 7 a comprehensive experimental program that was conducted in Israel to evaluate the consequences of a radiological dispersive device explosion.

### **1.6.2 Section 2: Security Consideration for Modes of Transportation**

The second section includes seven chapters presenting the vulnerability of the various modes of transport. It describes and evaluates security consideration of public transportation, airports, seaport, railroads, and pipelines.

This section starts with Chapter 8, authored by Wachs et al., which describes and categorizes security risks and prevention tactics in public transport systems on streets and amid mixed traffic that include stations and exclusive rights-of-way. Similar prevention strategies are addressed to terrorism and common criminal activities. In Chapter 9, Plant and Young illustrate threats and vulnerabilities to passenger and rail freight operations. Key policies and programs designed to address these security issues with an emphasis on the role of the DHS, information sharing, and public-private partnerships are discussed. In Chapter 10, Pandolfi considers steps that can be taken to improve or to change the security management in order to advance the overall operations of the American freight railroad system. Then, Poole discusses in Chapter 11 productive resource allocation in homeland security, with a primary focus on measures implemented at airports to protect passengers and planes. The chapter compared and contrasted US airport security policies and practices with those of Canada and the European Union. It also discusses whether it is feasible to use forms of cost-benefit analysis and cost-effectiveness analysis for resource allocation on a risk-based basis and explores the question of who should pay for airport security. In Chapter 12, Price and Hashemi introduce seaport operations, port and security infrastructure, shipping container logistics, and the need to secure the ports with minimum cargo disruption. Security strategies and technology are examined, along with a “great debate” on nonintrusive scanning of all or only high-risk containers. In Chapter 13, Inman and Morris discuss the Transportation Worker Identification Card (TWIC) program compliance as a mean to help secure the nation’s vital maritime transportation infrastructure, problems, evaluation, and the role of privatization. In Chapter 14, Polydoropoulou and Tsirimpa analyze port users’ attitudes and perceptions regarding security threats, as well as modeling travelers’ choice of port under alternative security scenarios, based on a case study for the island of Chios in Greece. The section ends with Chapter 15 by Talarico et al. who investigate security issues related to the pipeline systems. Traditional and advanced security measures used in pipelines are presented as well as future developments of new emerging technologies and recent applications. They also provide a support decision model aimed at

increasing the effectiveness of the set of selected countermeasures for the pipeline infrastructure security within a limited budget.

### **1.6.3 Section 3: The Role of Transportation in Evacuation**

This section includes three chapters dealing with the role of transportation in evacuation as a supporting response operations in large national disasters. The section starts with Chapter 16, authored by Daniel Hess and Christina Farrell who explore the factors and outcomes of mandatory and nonmandatory evacuation related to non-noticed and limited noticed disasters in nonurban settings with the purpose of improving evacuation policy and planning. Two examples—bushfires (in 2009) in Victoria, Australia, and a nuclear accident (in 2011) in Fukushima, Japan—are provided. In Chapter 17, David Heller discusses how better evacuation plans and procedures can significantly reduce hurricanes and other natural disaster impacts, based on lessons learned from Katrina (in 2005), Rita (in 2005), Irene (in 2011), and Sandy (in 2012), all in the United States. The section ends with Chapter 18 by Jaydeep Chaudhari et al. focusing on how public transportation can perform multiple roles and can be an effective partner in the four tasks of emergency management planning: mitigation, preparedness, response, and recovery. The chapter discusses how adequately transit systems are prepared and the challenges and issues that may arise in the event of an emergency evacuation.

## **1.7 CONCLUSION: RESOURCE ALLOCATION AND POLICY IMPLICATION**

Transportation systems including airports, airlines, water ports, ships, highways, pipelines, buses, rail, and mass transit are inherently vulnerable to different types of terror attacks. Bus, rail terminals, and airports generally include masses of people. Since the terrorists' goal is to inflict a major impact, such infrastructures are perceived by terrorist as "efficient" targets to hurt any civilization at its "soft belly." Therefore, it is likely to assume that transportation systems will continue to be a prime terrorist target. While bombing is the most common, the threats are various: biological, chemical, nuclear (dirty bombs), and cyber.

Terrorist access to major public transportation targets is relatively easy in comparison to power, water, and other infrastructures. Transportation systems should be highly accessible and accordingly are usually open to people, while access to other critical infrastructure is limited and can be easier guarded. In this regard, the aviation security model and its security procedure in the post-9/11 era are not applicable to surface transportation, which cannot be protected in the way commercial aviation is protected. Current technologies are still limited in detecting explosives or individuals who might approach critical points in targeted areas to inflict maximum damage. Maritime commerce in containers involves hundreds of thousand a year. Many of these containers move through several water ports before reaching the US harbor. Existing technologies do not allow thorough checking of these containers even though undetected

dirty bombs cause a high threat. These containers are often immediately transferred to trucks for transit to various US destinations where the explosion may occur.

Even highly sophisticated infrastructure protection could be ineffective for a few high-impact attacks. Thus, resources are better spent on response, preventing aftermath damages, and recovery efforts than on deterring and physical prevention measures. Operating transportation systems are essential for recovery efforts and the longer-term economic and social return to normal state. Thus, targeting transportation facilities prolongs recovery.

Review of major terror attacks suggests that certain types of attacks are “preferred” by terrorists since they are considered “more fit” or “more legal.” It cannot be ignored that most devastating global terrorist attacks have been perpetrated in the name of Islam, and as Bar discusses in Chapter 2, the body of Islamic rulings relating to justification of modern mass killing of civilians serves as the guideline for many Islamic terror acts. Bar concludes in his chapter that to combat the radical trend in Islam, what may be necessary is a “Kulturkampf” of the orthodoxy against the radicals, but in the short run, the Western political and legal arsenal needs to adapt itself to the existence of a religious war.

Transportation systems are essential for evacuation when a terrorist attack, a natural disaster, or a man-made failure occurs.

Efficient and effective evacuation can significantly mitigate the catastrophe consequences and therefore serves as one of the most promising means to response and recovery from such destructive incidents. Large-scale evacuation utilizes existing transportation infrastructure, requiring early and continuous planning and training and a well-managed and well-coordinated process once an evacuation starts. In this regard, multimodal transportation networks for emergency evacuation scenarios should also be in the forefront. In the case of public transit users, for example, school bus systems, especially in rural areas, are ideal for providing evacuation. As discussed by Chaudhari et al. in Chapter 18, school buses should be incorporated into a local emergency management plan. Hess and Farrell in Chapter 16 suggest that oversight of emergency planning by national and state governments is justified; however, local leaders are usually best positioned to manage disaster preparedness, response, and recovery efforts. Furthermore, evacuation procedure will benefit from innovations in communication network, social media, and joint operation centers. As stated in this chapter, an effective emergency response system must have resilient methods of communication and consistent messaging, as communication is often the first system to fail in the chaos of extreme events.

Five major reasons prevent socially optimal allocation of resources for homeland security services. First, government’s monopolistic position in the delivery of emergency services impedes efficient homeland security services. Second, “peak time demand” exists for emergency personnel and equipment. Third, rigid territorial boundaries of localities and states dictate the availability of personnel and equipment and often prevent efficient efforts. Fourth, perceived low probability of occurrence and high cost discourage appropriate spending. A fifth reason is the desire by officials to avoid mistakes. In the case of disasters, this means taking actions prematurely could be clearly shown to be a mistake so the cautious behavior approach is to wait

until the disaster is imminent. The objective is for households, business leaders, and government officials to take the long-term view. Achieving the socially desired spending should be addressed by the provision of appropriate incentives.

Profit-motivated businesses would be expected to take the more socially appropriate action as they evidently did in the case of Katrina (Sobel and Leeson 2006). Contracting out addresses the problem of inefficiency of monopolistic government. Some private guards could be deputized when an emergency occurs to fulfill temporary duties of law enforcement agents. Volunteers can be used for such semiskilled tasks. At times of disaster, similar equipment in the private sector may be idle. Registry of all public and private equipment should be prepared along with clear delivery options, leasing agreement, and payments.

The success of establishing a new organization for homeland security depends on few factors. First, it should not be an addition to existing public entities but rather should replace them. Second, public budgets for homeland security should be directed to the newly created regional entity. Third, the state should provide a legal foundation to the regional entity to sign contracts with public, private, and volunteer organizations. Fourth, when a disaster condition is announced, all powers and responsibilities are shifted from the various government agencies involved in first response and related services to the regional entity. Fifth, this new entity should not be constrained by government rules and regulations.

## REFERENCES

- Abrams, M. and Weiss, J. 2000. Malicious control system cyber security attack case study—Maroochy water services, Australia. Available at [http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study\\_report.pdf](http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf). Last visited October 17, 2014.
- Bar, S. 2004. The religious sources of Islamic terrorism. *Policy Review*, 125: 27–37.
- Blackstone, E.A. and Hakim, S. 2013. Competition versus monopoly in the provision of police. *Security Journal*, 26(2): 157–179.
- Blodget, H. 2012. We need to stop maximizing profit. *Business Insider*, December.
- Boaz, D. 2005. Catastrophe in big easy demonstrates big government's failure. *Commentary*, September 19. Available at <http://www.cato.org/publications/commentary/catastrophe-big-easy-demonstrates-big-governments-failure>. Last visited October 20, 2014.
- Bureau of International Security and Nonproliferation. 2014. Proliferation security initiative participants. US Department of State, Washington, DC, June 14. Available at <http://www.state.gov/t/isn/c27732.htm>. Last visited October 20, 2014.
- Business Executives for National Security (BENS). 2006, November. Regional public–private partnerships: The next wave in homeland security. BENS, Washington, DC.
- Butterworth, B.R., Dolev, S., and Jenkins, B.M. 2012. Security awareness for public bus transportation: Case studies of attacks against the Israeli public bus system. Report no. 11-07. Mineta Transportation Institute, San Jose State University, San Jose, CA.
- Carafano, J.J. 2012. Next step for transportation security. Testimony before Subcommittee on Transportation Security, Committee on Homeland Security, US House of Representatives, September 11.

- Edwards, F.L. and Goodrich, D.C. 2014. Exercise handbook: What transportation security and emergency preparedness leaders need to know to improve emergency preparedness. Report no. CA-MTI-14-1103. Mineta Transportation Institute, San Jose State University, San Jose, CA.
- Elias, W., Albert, G., and Shiftan, Y. 2013. Travel behavior in the face of surface transportation terror threats. *Transport Policy*, 28: 114–122.
- Exel, N. and Rietveld, P. 2001. Public transport strikes and traveller behaviour. *Transport Policy*, 8(4): 237–246.
- Floyd, M., Gibson, H., Pennington-Gray, L., and Thapa, B. 2004. The effect of risk perceptions on intentions to travel in the aftermath of September 11, 2001. *Journal of Travel and Tourism Marketing*, 15(2–3): 19–38.
- Holguin-Veras, J., Paaswell, R.E., and Yali, A.M. 2003. Impact of extreme events on intercity passenger travel behavior: The September 11th experience. TRB 2003 annual meeting, challenges. *Homeland Security Affairs*, 8(October): Article 18.
- Homeland Security News Wire. 2011. Counterterrorism financing: Analysts question wisdom of DHS spending, May 20. Available at <http://www.homelandsecuritynewswire.com/analysts-question-wisdom-dhs-spending>. Last visited October 10, 2014.
- Jackson, O. 2008. The impact of the 9/11 terrorist attack on the U.S. economy. March 3. Available at <http://www.journalof911studies.com/volume/2008/OliviaJackson911andUS-Economy.pdf>. Last visited October 10, 2014.
- Janczewski, L.J. and Colarik, A.M. 2008. *Cyber warfare and cyber terrorism*. IGI Global, Hershey, PA.
- Jenkins, B.M. 2001. Protecting public surface transportation against terrorism and serious crime: An executive overview. Report no. 01-14. Mineta Transportation Institute, San Jose State University, San Jose, CA.
- Jenkins, B.M. July 2003. *Improving public surface transportation security: What do we do now?* The Lexington Institute, Arlington, VA.
- Johnston, W.R. 2010. Chronology of terrorist attacks in Israel: Introduction. Available at <http://www.johnstonsarchive.net/terrorism/terrirsrael.html>. Last visited October 24, 2014.
- Kirschenbaum, A. 2006. Terror, adaptation and preparedness: A trilogy for survival. *Journal of Homeland Security and Emergency Management*, 3(1): 23–48.
- Kunreuther, H., Michael-Kayan, E., and Pauly, M. 2013. Making America more resilient toward natural disasters: A call for action. *Environment*, 55(4): 15–23.
- Lieberman, J. 2005. Hurricane Katrina: What can government learn from the private sector's response. Presentation at the US Senate, November 16. <http://www.hsgac.senate.gov//imo/media/doc/111605JILOpen.pdf?attempt=2>. Last visited October 6, 2014.
- Matusitz, J. 2005. Cyberterrorism. *American Foreign Policy Interests*, 2: 137–147.
- Michael-Kayan, E. and Kunreuther, H. 2012. Paying for future catastrophes. *New York Times, Sunday Review*, November 24.
- MIPT. 2007. *The MIPT annual 2006*. National Memorial Institute for the Prevention of Terrorism, Oklahoma City, OK.
- Moynihan, D.P. 2009. *The response to hurricane Katrina*. In *Risk governance deficits: An analysis and illustration of the most common deficits in risk governance (Report)*. International Risk Governance Council, Geneva. Available at [http://irgc.org/wp-content/uploads/2012/04/Hurricane\\_Katrina\\_full\\_case\\_study\\_web.pdf](http://irgc.org/wp-content/uploads/2012/04/Hurricane_Katrina_full_case_study_web.pdf). Last visited October 10, 2014.

- Nissenbaum, H. 2005. Where computer security meets national security. *Ethics and Information Technology*, 7(2): 61–73.
- Nissenbaum, H. and Hansen, L. 2009. Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, 53: 1155–1175.
- Nowacki, G. 2014. Threat assessment of potential terrorist attacks to the transport infrastructure. *TransNav*, 8: 219–227.
- Polzin, S.E. 2002. Security considerations in transportation planning. A white paper prepared for the Arizona Department of Transportation. Southeastern Transportation Center.
- Potoglou, D., Robinson, N., Chong, W.K., Burge, P., and Warnes, R. 2010. Quantifying individuals' trade-offs between privacy, liberty and security: The case of rail travel in UK. *Transportation Research Part A*, 44: 169–181.
- RAND Database of Worldwide Terrorism Incidents. 2014. Terrorism incidents database search. Available at [http://smapp.rand.org/rwtid/search\\_form.php](http://smapp.rand.org/rwtid/search_form.php). Last visited April 23, 2014.
- Rid, T. 2012. Cyber war will not take place. *Journal of Strategic Studies*, 35(1): 5–32.
- Roell, P. 2009. Maritime terrorism—a threat to world trade? Statement by Dr. Peter Roell at the International Conference on Comprehensive Security in the Asia-Pacific Region, November 30–December 1, 2009, Tokyo, Japan.
- Ronchi, E., Colonna, P., Capote, J., Alvear, D., Berloco, N., and Cuesta, A. 2012. The evaluation of different evacuation models for road tunnel safety analyses. *Tunnelling and Underground Space Technology*, 30: 74–84.
- Sandler, T. and Enders, W. 2004. An economic perspective on transnational terrorism. *European Journal of Political Economy*, 20(2): 301–316.
- Shepherd, W.G. and Shepherd, J.M. 2004. *The economics of industrial organization*. Waveland Press, Long Grove, IL.
- Sobel, R.S. and Leeson, P.T. 2006. Government's response to hurricane Katrina: A public choice analysis. *Public Choice*, 127: 55–73.
- Steen, M. 2014. Volunteer force: How to recruit, retain and organize volunteers. *Emergency Management*, September: 23–25.
- Szylionwicz, J.S. and Zamparini, L. 2013. *Maritime security: issues and challenges*. In *Maritime transport security* (Eds. Bichou, K., Szylionwicz, J.S., and Zamparini, L.). Edward Elgar Publishing, Glos: 13–23.
- Tabansky, L. 2011. Basic concepts in cyber welfare. *Military and Strategic Affairs*, 3(1): 75–92.
- Theroux, M.L.G. 2005. Public and private responses to Katrina: What can we learn? The Independent Institute, October 20. Available at <http://www.independent.org/newsroom/article.asp?id=1589>. Last visited October 7, 2014.
- US Senate. 2006. Hurricane Katrina: A nation still unprepared. Special Report of the Committee on Homeland Security and Governmental Affairs. Special Report 109-322. Available at <http://www.gpo.gov/fdsys/pkg/CRPT-109srpt322/pdf/CRPT-109srpt322.pdf>. Last visited October 13, 2014.



## **SECTION I**

---

### **MOTIVATION AND CHALLENGES**



---

# 2

---

## TERRORIST TARGETING OF PUBLIC TRANSPORTATION: IDEOLOGY AND TACTICS

SHMUEL BAR

*Samuel Neaman Institute for National Policy Studies, Technion Israel Institute of Technology,  
Haifa, Israel*

*And prepare against them whatever you are able of power...by which you may  
terrify the enemy of Allah and your enemy...whatever you spend in the cause of  
Allah will be fully repaid to you...*

Koran 8:60

### 2.1 BACKGROUND

Many of the most spectacular terrorist acts in the last decades were perpetrated against—or using—mass public transportation such as aircrafts, trains, buses, and even cruise ships. In general, acts of terrorism against public transportation evolved since the 1970s from acts of hostage taking with predefined goals of freeing imprisoned terrorists to acts of indiscriminate murder of passengers. In order to understand the strategic and ideological aspects of terrorism against public transportation, it is necessary first to understand the religious beliefs and the historic development of this terrorist modus operandi.

## 2.2 THE HISTORY OF TERRORIST-MOTIVATED HIJACKING

Hijacking of commercial aircraft began in the early 1960s with hijacking to Cuba. However, individuals whose goal was to divert the aircraft to Cuba carried out most of these hijackings. While these actions did cause certain disruption of air transportation, there was little or no concern that the hijackers would intentionally kill other travelers.

The ease of such actions was quickly picked up by terrorist organizations. The initial acts of “skyjacking” were carried out by various factions of the Palestinian Liberation Organization (PLO) with the goal of freeing their comrades in Israeli and other jails. The hijackings of civil aviation targets during the 1960s and 1970s (~20 attacks) by Palestinian organizations were all directed toward such a goal. The vulnerability of air travel made “skyjacking” a popular modus operandi for a wide range of terrorist organizations. However, many of these attempts ended in rescue operations that underlined the extents that Western nations were willing to go to in order not to succumb to such extortion. Cases of hijacking aircraft with the goal of freeing prisoners during the 1970s and 1980s included the Sabena airliner hijacked to Israel (May 1972); the Air France flight that was diverted to Entebbe, Uganda (June–July 1976), and freed by Israeli commandos; and Lufthansa 181 that was diverted to Mogadishu (October 1977) and freed by West German commandos. Interestingly, most of these hijackings or hijacking attempts were perpetrated against European or Japanese aircraft, while attacks on the Israeli airline—El Al—were for the most part attempts to bomb the aircraft or directly attack it on the ground.<sup>1</sup>

Hijackings, however, were not the only terrorist threat to civil aviation. A number of attacks were carried out against aircraft on the ground or by infiltration of explosives into aircrafts and exploding them in flight. The attack by members of the Japanese Red Army (JRA) at Lod International Airport in Israel (May 1972) was, in this sense, exceptional insofar as the terrorists did not carry the arms on them during the flight but in the luggage, opened them upon arrival, and opened fire upon arrival at the airport. These attacks did not follow the political logic of hijackings for the sake of freeing prisoners.

The material benefit from airline hijacking also became an important incentive. The growing popularity of hijacking of aircraft by terrorist organizations was enhanced by the lack of a robust response by the target countries and their willingness to give in to demands both regarding freeing imprisoned terrorists and in payment of actual blackmail. The very specter of such actions alone was exploited by terrorist organizations to extort additional concessions from affected countries. During the 1970s, for example, the government of France paid the Abu Nidal Organization (ANO) annual sums through the Saudi government in order to exclude French targets from the terrorist acts of that group. In February 1972, Lufthansa paid

<sup>1</sup>El Al Flight 253, was a Boeing 707 en route from Tel Aviv, Israel, to New York City, United States, when it was attacked by two Arab militants as it was about to depart from a layover in Athens, Greece, on December 26, 1968. One passenger was killed. The terrorists were apprehended by the Greek authorities, sentenced, and freed after a few months.

the PLO a ransom of \$5 million, but the highest hijacking ransom (\$6 million) was paid by the Japanese government to the hijackers of a JAL flight with 38 hostages at Dhaka airport in Bangladesh in October 1977. Arguably the most blatant cynical use of aircraft hijacking to strike a deal with terrorists was the hijacking of Lufthansa to Zagreb in October 1972. On October 29, 1972, 7 weeks after the 1972 Olympic Munich massacre of 11 Israeli athletes, a Lufthansa flight left Damascus, Syria, bound for Frankfurt, Germany, with a stop in Beirut. There were only 12 passengers on the flight. Two Black September terrorists boarded the plane and demanded to be flown to Munich. They called for the release of the three remaining Munich terrorists who were in West German jails. German Chancellor Willy Brandt immediately agreed, claiming that the passengers and crew were in a life-threatening situation. In fact, the German government, fearing further terrorist attacks on German soil, struck a deal with Fatah, in which the hijacking was prestaged between German intelligence and the Palestinian organization in order to allow Germany to release the three terrorists.

Interestingly, most of these attacks were perpetrated by left-wing terrorist groups: the Palestinian Popular Front for the Liberation of Palestine (PFLP), the JRA, and the German Red Army Faction (RAF). The PFLP, as an orthodox Marxist movement, felt obliged to justify its actions within a Marxist-Leninist context. Hence, in justifying the targeting of airlines, ideologues of the PFLP generally claimed that they had not targeted civilians per se and were not intending to kill the hostages indiscriminately, but to use them to extract concessions from their enemies and to focus world opinion on the Palestinian problem. Its offshoot—the DFLP—on the other hand did not find in Marxist ideology justification for airline hijacking and excluded such actions from their terrorist repertoire, claiming that they only serve to bolster the Israeli propaganda against the Palestinians.

With the advent of Islamist terrorism on the stage of international terrorism, the motivation for aircraft hijacking changed. In 1985, the nascent Shiite organization—Hezbollah—also hijacked TWA 847 to Beirut and from there to Algiers. Demands by hijackers became more political and unrealistic, including demands for Israeli withdrawal from all the territories occupied in 1967 or withdrawal of all US forces from the Middle East. The 1985 hijacking though was not followed by a wave of similar attacks.

By the second half of the 1980s, however, airline security had made infiltration into aircraft with firearms more and more difficult. It is possible that the shift from hijacking as a means to free prisoners to attempts to blow up aircraft in flight was due to the effectiveness of countermeasures that were developed to prevent the infiltration of firearms into aircraft and the decrease in the willingness of countries to give in to such demands. During the mid-1980s, attacks on aircraft began to evolve from hijacking into attempts to destroy civilian aircraft in flight and ground attacks on soft airline-related targets.

During the 1980s, Libya initiated a series of attacks on aircraft. These included attacks by its Palestinian proxy organization, the ANO, against an EgyptAir Flight 648 (1986) that was landed in Malta and stormed by Egyptian commandos with a high price of 58 killed out of 90 passengers and three attacks on check-in areas: the

El Al check-in counters at Leonardo da Vinci di Fiumicino International Airport in Rome, Vienna International Airport, and the Pan Am check-in at Karachi International Airport in Karachi, Pakistan. Later (1988), Libyan intelligence directly engineered the bombing of Pan Am 103 that crashed over Lockerbie, Scotland, and of the French UTA 772 that was exploded over Niger. The Iraqi proxy Abu Ibrahim faction of the PFLP/SC (formerly under Wadi' Haddad—who had orchestrated the Entebbe hijacking) prepared a number of suitcase bombs with barometric fuses that were set to explode when the aircraft reached a given altitude. Western intelligence agencies conducted an extensive chase during 1982 to locate and defuse the suitcases. None of them exploded; however, these attempts adumbrated later terrorist attacks that succeeded. Subsequently, in April 1986, Syrian intelligence dispatched a Jordanian agent to infiltrate a bomb cached in a radio set to an El Al flight from London Heathrow airport to Tel Aviv. The bomb was given by the Jordanian Nezar Hindawi to his pregnant girlfriend, ostensibly as a gift to his “family” in the West Bank and was set to explode as the plane reached a given altitude. The Israeli security screening foiled the plot. While Libya eventually acknowledged its responsibility for a number of attacks and paid reparations, none of these states have ever provided an ideological justification for their actions.

During the 1990s, the number of attacks on airlines decreased. It appears that the drop in attempts to hijack aircraft for the sake of freeing prisoners lowered the guard of many Western nations and paved the road to 9/11. While it is clear that US intelligence agencies had not seriously taken into account hijacking of aircraft in order to crash them into populated areas, such use of a hijacked aircraft was taken into account years previously in Israel. The Israeli Air Force implemented as early as the mid-1970s a standing operation procedure (code named “Host of Heaven”) that included standing operation procedures to prevent any hijacked civil aircraft from approaching airspace over populated areas. The procedure went as far as to authorize interception of such civilian aircraft if they approached populated areas.

By 1985, however, Fatah, the PLO’s largest faction, renewed its involvement in international terrorism by hijacking the cruise liner Achille Lauro and murdering Jewish-American passenger Leon Klinghoffer. This event however was basically in line with previous attempts to hijack aircraft for exchange of prisoners.

During the 1990s and early twenty-first century, attacks on aircrafts gave way to attacks on trains and other forms of public transportation. This may have been due to a perception that aircraft security had improved and that the capability of authorities to monitor access to mass ground transportation was limited. The attacks on the Tokyo Underground in 1997, the attacks of 7/7 against the London Underground in 2005, and the attacks on the Atocha Madrid train station in 2004 are such examples. In the years following the Oslo Agreement (1993–1996) and during the “Intifada” of 2001–2004, Palestinian terrorists carried out numerous attacks on Israeli buses. The enhanced security on airlines certainly diverted attention to other means of mass transportation, where security measures such as X-ray machines and metal detectors could not be applied. The logic behind the attacks remained the same—to hit Western society at its “soft belly” and to create a sense of insecurity.

## 2.3 ISLAMIC JUSTIFICATION FOR ATTACKS ON MASS TRANSPORTATION

Islamist terrorists adhere to similar strategic and tactical considerations like their secular predecessors. However, in addition to those considerations, they are obliged to take into account the rulings of Islamic law (*Shari'ah*). Decisions regarding actions that may otherwise be “illegal” in normal circumstances (i.e., indiscriminate murder of hostages) cannot be decided by abstract morality or by politics, but by meticulous legal analysis according to the *Shari'ah*. Obviously, the individual “lay” Muslim is not qualified to decide such matters. It is the role of the authoritative scholar (‘Alem, pl: ‘Ulama) to provide a legal ruling (fatwa) to guide the believers (Bar, 2006).

The fatwa in Islam is a legal ruling based on the Koran, the hadith (oral traditions relating to the life of the Prophet Muhammad), and other legal instruments such as analogy, public interest, etc. The idea behind the fatwa is that Islam encompasses the entire life of the Muslim, and he does not have the tools to know what is correct and what is not. Therefore, he is obliged to rely on religious scholars to inform him of what is right and what is wrong. Ultimately, if a Muslim obeys a fatwa provided by a religious scholar with appropriate qualifications, he is exempt from personal accountability for his actions. The question remains, however, what the appropriate qualifications are. In the past, the regimes held control over the religious establishments and those had a monopoly over issuance of fatwas. However, during the last decades, there has been a process of “devolution” of authority to lower level—and sometimes self-declared—religious scholars who arrogate to themselves the right to issue fatwas.

The use of fatwas to call for certain action became known in the West as a result of Osama Bin Laden’s 1998 fatwa against the United States and Israel. The political strength of these fatwas has been time tested in Muslim political society by rebels and insurgents from the Arabian Peninsula to Sudan, India, and Indonesia. The fatwas promulgated by Sheikhs and ‘Ulama affiliated with radical Islamist organizations, therefore, play a pivotal role in the ostensibly tactical decisions relating to targeting of mass transportation. These fatwas must determine whether it is permitted to kill noncombatant civilians—women, children, elderly, clerics, and “prisoners” (passengers of a plane taken hostage may be construed as such)—or “protected” non-Muslims in Muslim countries. They must also legitimize suicide attacks as a form of Jihad in the light of the severe prohibition for a Muslim to take his own life.

From this point of view, the considerations of terrorist organizations regarding choice of transportation-related targets are quintessentially rational. The desired end result is, according to Abu Musab al-Suri (Mustafa Setmariam Nasar), one of the most prominent ideologues of the modern jihadi movement, to inflict the greatest degree of harm on the enemy. In his book *The Call for a Global Islamic Resistance* (December 2004), he calls for attacks on a series of key targets in the United States, among them public transportation.<sup>2</sup> In his writings, he expresses regret that the

<sup>2</sup>“The Call for a Global Islamic Resistance,” December 2004.

aircraft that were hijacked on 9/11 did not carry weapons of mass destruction,<sup>3</sup> so they could inflict greater damage. Abu Musab al-Suri developed a practical strategy based on attacks on mass transportation. He was accused of planning the London Underground bombings (7/7/2005), killing 52 people and injuring more than 700 others, and the Madrid attacks in 2004. In a statement released after the attacks, he said: “[In my teachings] I have mentioned vital and legitimate targets to be hit in the enemy’s countries… Among those targets that I specifically mentioned as examples was the London Underground. [Targeting this] was and still is the aim.”

The logic of disrupting the Western economy—and not necessarily causing maximum casualties—though seems to be more predominant in the minds of some jihadi strategists. For example, Anwar al-Awlaki (the most prominent jihadi thinker from the United States) explained the value of bombing planes in terms of creating a sense of insecurity that would necessitate enormous investments in order to prevent further attacks of the same type. For example:

In the name of Allah, the Most Compassionate, the Most Merciful. From Usama to Obama: peace be upon he who follows the guidance. As for what comes after: if our messages to you were conveyed by words, we wouldn’t send them to you on airplanes; and the message meant to reach you by way of the airplane of the mujahid hero Umar al-Farouk—may Allah release him—is a underlining of a previous message which the heroes of the 11th [of September] brought to you, and which has been reiterated both before and since: namely, that America will never dream of security until we actually experience it.<sup>4</sup>

This is reiterated in more detail in the issue of Inspire (Fall 1431):

To the American people I say: Do you remember the good old days when Americans were enjoying the blessings of security and peace? When the word “terrorism” was rarely invoked, and when you were oblivious to any threats? I remember a time when you could purchase an airline ticket from the classified section of your local or college newspaper, and use it even though it was issued to a different name because no one would bother asking you for an ID before boarding a plane. No long lines, no elaborate searches, no body scans, no sniffing dogs, no taking off your shoes and emptying your pockets.<sup>5</sup>

The bombing of freight planes was also viewed in the context:

Since 9-11 the West has been stepping up defenses for its commercial aircrafts. The continuous attempts that followed 9-11 by our brother Richard Reid,<sup>6</sup> the Heathrow

<sup>3</sup> “I feel sorry because there were no weapons of mass destruction in the planes that attacked New York and, Washington on 9/11. We might have been relieved of the biggest number possible of voters who elected Bush for a second term!” Statement attributed to Abu Musab al-Suri on jihadi websites, January 25, 2005.

<sup>4</sup> *Inspire*, Fall 2010.

<sup>5</sup> *Inspire*, Summer 2008.

<sup>6</sup> Richard Reid, “the shoe bomber,” is a British citizen who attempted to detonate American Airlines Flight 63 from Paris to Miami, wearing shoes packed with explosives.

airport plot and finally the operation of brother Umar Farouk<sup>7</sup> have forced the West to spend billions of dollars to defend its airplanes. But what about cargo planes?... The air freight is a multi-billion dollar industry. FedEx alone flies a fleet of 600 aircrafts and ships an average of four million packages per day. It is a huge worldwide industry. For the trade between North America and Europe air cargo is indispensable and to be able to force the West to install stringent security measures sufficient enough to stop our explosive devices would add a heavy economic burden to an already faltering economy. We knew that cargo planes are staffed by only a pilot and a co-pilot so our objective was not to cause maximum casualties but to cause maximum losses to the American economy. That is also the reason why we singled out the two U.S. air freight companies: FedEx and UPS for our dual operation.<sup>8</sup>

Another motif is the employment of attacks on transportation in order to hit at the local particular interests of the “weak link” in the Western alliance to cause it to disintegrate. A document published a few months before the attacks in Madrid entitled “The Jihad of Iraq—Hopes and Dangers” (Iraq al-Jhad—Amal wa-Akhtar) determines that military force alone will not chase the United States out of Iraq, and economic and political pressure is necessary. Political pressure can be brought to bear through reducing the number of American allies in Iraq. The document analyzes the domestic situation in three countries that have forces in Iraq—the United Kingdom, Spain and Poland—and proposes to pressure the first two through attacks in their own territory. The document was published before the attacks in Madrid and London.<sup>9</sup>

The issue of attacks on public transportation relates to the directions in Islamic law of jihad regarding hostages or prisoners of war. Once the aircraft, boat, or train has been hijacked, the passengers are deemed “prisoners.” The principles that affect the religious thinking in this respect include<sup>10</sup> the injunction that prisoners can only be taken after the enemy has been defeated (i.e., if the passengers are “hostile infidels,” they can be killed). However, in general, Islamist ideologues, based on the Koran (47:4),<sup>11</sup> leaves the decision whether to kill the passengers or to hold them for ransom (prisoner exchange) to the discretion of the Imam in charge of the Jihad. As authority for this position, modern Islamist writers tend to refer to the leader of the mujahideen in Afghanistan during the war against the Soviets, Sheikh Abdallah Azzam who left the fate of “prisoners” in the hands of the Imam, who may decide according to the interest of the Muslims whether to free them or to allow them to

<sup>7</sup>Umar Farouk Abdulmutallab, popularly referred to as the “underwear bomber,” is a Nigerian man who attempted to detonate plastic explosives hidden in his underwear on Northwest Airlines Flight 253, en route from Amsterdam to Detroit, Michigan, on December 25, 2009.

<sup>8</sup>Inspire, No. 3, November 2010.

<sup>9</sup>See “Media Committee for the Victory of the Iraqi People (Mujahidin Services Centre),” pp. 25–33.

<sup>10</sup>Fatwa: Sheikh Yusuf al-Qaradawi, “Enslavement of POWs,” May 26, 2004. <http://www.islamonline.net/fatwa/english/FatwaDisplay.asp?hFatwaID=114759>; Fatwa: by a group of Muftis, “Islam’s Stance on Prisoners of War,” June 1, 2003, <http://www.islamonline.net/fatwa/english/FatwaDisplay.asp?hFatwaID=55158>

<sup>11</sup>According to the Koran 8:67, “It is not fitting for a Prophet that he should have prisoners of war until he has thoroughly subdued the land,” and 47:4, “So when you meet in battle the *kuffar*, then smite the necks until when you have overcome them, then make [them] prisoners, and afterwards either set them free as a favor or let them ransom [themselves] until the war terminates.”

ransom themselves. Later, the “Secret Islamic Army—the Battalions of the Black Banners” (*Al-Jaish al-Islami al-Siri—Kataib al-Ra’yat al-Sud*)—requested a fatwa from the Iraqi Sunni Association of Muslim Scholars (*Jama’at al-‘ulam’ al-Muslimin*) on the issue of permissibility of killing kidnapped foreigners.<sup>12</sup>

Another related “legal” issue that comes up in jihadi discussions regarding mass terrorist attacks is the principle in jihad of “revenge” (*qisas*) and “eye for an eye” (*mu’amala bil-mithl*). Jihadi ideologues point out that according to traditional Islamic Shari’ah (religious law), the value of the life of a Muslim is greater (between 2 and 10 times) than that of an infidel.<sup>13</sup> Thus, they conclude that according to the number of Muslims all over the world killed by the infidels under American leadership, Muslims have the right to kill at least four million Americans, half of them children.

Not all jihadist strategists support this view. In the wake of 9/11, Islamic establishments in Muslim countries and in the West issued a number of statements of condemnation and *fatwas*. The head of the Supreme Council of ‘Ulama of Saudi Arabia, Sheikh Saleh bin Mohammed al-Lahidan, enumerated in the context of his response to 9/11 (in his fatwa of September 14, 2001) a list of relevant sins that are all forbidden in Islam: injustice among humans; aggression against those who have committed no crime; killing of innocent people, the weak, infants, women, and the elderly; destroying property; mischief (corruption); and laying waste to the land.<sup>14</sup> The radical Sheikh, Yusuf Qaradawi (September 12, 2001), also issued a *fatwa* refuting the Islamic legitimacy of the attacks, pointing out that Islam does not permit indiscriminate killing of innocent with the guilty, since “no one may carry the burden of the other.” Therefore, if the act was truly perpetrated by a Muslim, “we condemn and incriminate him in the name of our religion and our law and he deserves the lawful deterrent punishment.”<sup>15</sup>

On September 17, 2001, a week after the attacks, the mufti of Saudi Arabia, Sheikh ‘Abd al-‘Aziz Aal al-Sheikh, issued his own *fatwa* regarding the attacks. They were described as “actions that *Shari’ah* does not sanction” and “not from this religion.” His ruling was based on the principle that “no person can bear the burden of another.” Hijacking of planes and mass murder are a form of “injustice, oppression and spreading of corruption on earth,” which even hatred does not justify. A similar position was taken by Sheikh Salih as-Suhaymee (October 18, 2001), who based his condemnation of the attacks on defining them as *fahsh*. Such acts include illegal sexual acts, disrespect of parents, polytheism, and killing without reason. Since Allah has forbidden the killing of non-Muslims who have a treaty with the Muslims (*mujahideen*), women, children, the elderly, and monks, and the cutting down of trees (destruction of fruit-bearing property), the attacks of September 11 were not permissible (*ghayr ja’iz*).<sup>16</sup> The opposition to attacks on public transportation did extend to some jihadi circles, such as Abu Basir al-Tartusi, a Syrian jihadist who lives

<sup>12</sup> *Al-Watan* (Saudi Arabia), September 6, 2004; *The Guardian* (UK), September 5, 2004.

<sup>13</sup> Yohanann Friedmann, *Tolerance and Coercion in Islam: Interfaith Relations in the Muslim Tradition*, Cambridge University Press, Cambridge, NY, 2003, pp. 39–47.

<sup>14</sup> The *fatwa* is translated on the website of The Islamic Center, Washington, DC. <http://www.theislamiccenter.com/AlNur.5.02/judicial.html>

<sup>15</sup> *Fatwa*: Sheikh Yusuf al-Qaradawi and others, September 12, 2001.

<sup>16</sup> *Fatwa*: Sheikh Saalih as-Suhaymee, October 18, 2001. <http://www.fatwa-online.com/news/0011018.htm>

in London, who issued (July 9, 2005) a fatwa refuting the Islamic legitimacy of the London bombings. However, the fact that he lives in London may have had some weight in his decision to issue the fatwa.

## 2.4 CONCLUSION

The discussion in this chapter does not cover all the considerations that may arise in the tactical thinking of terrorists regarding targeting public transportation. Strictly speaking, a military or terrorist leader will choose a course of operation or a target according to a matrix that integrates operational feasibility, quality, and scope of the results (both in terms of numbers of casualties among the enemy and the psychological and economic effect); the cost of the effort (in terms of the perpetrator's human and financial resources); and the cost of failure. However, once a course of action has been identified, both military and terrorist leaders consider an additional factor—is the action counterproductive to the strategic goals of the organization, is it controversial within the reference group of the organization (cause mutiny or fractures in the line of command), and is it "legal"?

Military leaders in Western countries take this into account in decisions whether to use massive force against an identified enemy who is hiding among civilians, forcing them to calculate the scope of tolerable civilian casualties or "collateral damage." The terrorist leader, on the other hand, may be bound by religion or ideology to justify his actions. As was pointed out earlier, the DFLP, as a Marxist-Leninist organization, eschewed terrorist attacks outside of "Palestine" as contradictory to its ideology. In the context of modern Islamist terrorist, the body of Islamic rulings relating to justification of mass killing of civilians serves as the guideline for many of these organizations. Such rulings have also been issued in regard to use of weapons of mass destruction such as nuclear, biological, and chemical weapons.

The tactical appeal for terrorists of all ideological streams for attacking mass transportation will not disappear. Therefore, it remains to ask how such attacks can be deterred and how the very ideology that condones and even encourages such actions can be countered. The pluralistic nature of Islamic jurisprudence, however, implies that even if prominent moderate Sheikhs issue fatwas against such acts of terrorism, there will emerge others who will condone them.

To combat the radical trend in Islam, what may be necessary is a "Kulturkampf" of the orthodoxy against the radicals. To the Western ear, this may sound medieval and totally incompatible with principles of freedom of religion and expression. However, in the absence of an Islamic Reformation, it may be the only way to combat the *jihadi* movement from within Islam. In the meantime, the Western political and legal arsenal needs to adapt itself to the existence of a religious war. This calls for **criminalization** of acts and statements, even if based on scriptures, and **redefining the principle of personal criminal culpability** to cover religious leaders for the acts of their flock as a result of their spiritual influence. Such modifications may be problematic for Western legal systems; however, under the circumstances, such contradictions may be the lesser of the evils.

## REFERENCE

Shmuel Bar, *Warrant for Terror: Contemporary Fatwas and the Duty of Jihad*, Hoover Institution and Rowman & Littlefield, Lanham, 2006.

## FURTHER READING

Shmuel Bar, "The Religious Sources of Islamic Terrorism," *Policy Review*, Vol. 125, June/July, pp. 27–37, 2004.

Shmuel Bar, *Jihad Ideology in the Light of Contemporary Fatwas*, Hudson Institute, Center on Islam, Washington, DC. Monograph Series No. 1, Paper No. 1, August 2006.

Shmuel Bar, *The Conflict between Radical Islam and the West—Origins, Prognosis and Prescriptions*, The Institute for Policy and Strategy, Interdisciplinary Center, Herzliya, 2007a.

Shmuel Bar, "Deterring Non-State Terrorist Groups: The Case of Hizballah," *Comparative Strategy*, Vol. 26, No. 4, pp. 469–493, 2007b.

Shmuel Bar, "Deterring Terrorists—What Israel Has Learned," *Policy Review*, Vol. 149, 2008. <http://media.hoover-stage.org/publications/policy-review/article/5674> (accessed March 1, 2015).

Shmuel Bar, Center on Islam, Democracy and the Future of the Muslim World, *Sources of Islamist Strategic Thought*, Monograph Series No. 2, Paper No. 1, Hudson Institute, Washington, DC, August 2008.

Shmuel Bar, Shmuel Bachar, Rachel Machtiger, and Yair Minzili, *Establishment Ulama and Radicalism in Egypt, Saudi Arabia, and Jordan*, Monograph Series No. 1, Paper No. 4, Hudson Institute, Center on Islam, Washington, DC, December 2006.

---

# 3

---

## ON THE RATIONALITY AND OPTIMALITY OF TRANSPORTATION NETWORKS DEFENSE: A NETWORK CENTRALITY APPROACH

YANIV ALTSHULER<sup>1</sup>, RAMI PUZIS<sup>2</sup>, YUVAL ELOVICI<sup>3</sup>,  
SHLOMO BEKHOR<sup>4</sup>, AND ALEX (SANDY) PENTLAND<sup>1</sup>

<sup>1</sup>*Media Lab, Massachusetts Institute of Technology, Cambridge, MA, USA*

<sup>2</sup>*Deutsche Telekom Lab, Department of Information Systems Engineering, Ben-Gurion University, Beer Sheva, Israel*

<sup>3</sup>*Department of Information Systems Engineering and Telekom Innovation Laboratories, Ben-Gurion University, Beer Sheva, Israel*

<sup>4</sup>*Transportation Research Institute, Technion – Israel Institute of Technology, Haifa, Israel*

### 3.1 INTRODUCTION

Since the days of the Roman Empire, transportation networks have been one of the cornerstones for the strength and stability of states. Maintaining the availability of roads and the safety of travelers were always an important challenge for rulers and governments. Transportation systems in most of modern countries are considered nowadays relatively safe. However, maintaining their safety requires constant monitoring and law enforcement. With the increase in the complexity of transportation systems, combining various types of land, air, and marine vehicles, both private and public, the challenge of monitoring them becomes both increasingly difficult and important. In fact, attackers and disturbing factors that threaten transportation networks usually get to their destination using this network as well. For example, a

group of terrorists that are planning to carry out an attack (such as hijacking an airplane or exploding a subway station) will most likely get to their destination using some means of transportation. When it comes to their security profile, transportation networks, therefore, have a unique feature, being both a potential target for an attack and the mean to carry it.

Ideally, each transportation network (global, national, and urban) should have been built while incorporating a monitoring station alongside each of its routes and intersections. This, however, is not feasible due to privacy reasons and financial and operational considerations. It is hence crucial to find deployment schemes for monitoring stations, which would analytically guarantee the maximization of traffic monitoring, using a limited number of monitoring units. Such a scheme could be used to calculate either a static deployment of large-scale monitoring units or a dynamic on-demand deployment that could be implemented as an urgent response for a specific threat. Ultimately, this system would provide the maximal detection probability of threat agents for a specific budget or, alternatively, the minimal number of monitoring units for a predefined requested detection probability. These monitoring stations may be either police patrols; automatic units for detecting biologic, chemical, or radiologic hazards; or any other monitoring units.

In order to produce efficient deployment schemes, the traffic pattern of the users of the transportation system must be thoroughly studied. The analysis of mobility trends and demands forecasting in transportation networks relies nowadays heavily on household survey data that provides the required input for calibrating the mathematical models that represent decisions people make related to travel (Stopher et al. 2006). However, a well-known problem common to all interview-type surveys is nonresponse. Complex methods to correct for nonresponse have been developed; however, these alleviate the problem only partially (Richardson and Wolf 2001).

As mentioned in Bekhor et al. (2013), another limitation of household surveys is the need for active cooperation from the respondents, relying on their memory and patience. The need for active participation reduces the ability to capture complex travel and activity patterns and the ability to collect data over a long period of time. The problems mentioned earlier, coupled with budget constraints, explain the fact that typical household surveys collect data regarding a period of merely 1 or 2 days for each household. As a result, there exists a strong need for finding an alternative mechanism of assessing mobility and traffic demand in transportation networks, one that could be used without the necessary, tedious, and inaccurate process of surveying.

Combining this with the need for fast deployment optimization solutions, it is clear that in order to find an efficient optimization scheme that would satisfy all aspects of transportation-related homeland security deployment problem, we must resort to methods that rely on the analysis of the *transportation network* itself. Such a method can produce dynamic solutions to a variety of optimization systems and do so in close to real time (using efficient heuristic search methods).

*Betweenness centrality* (BC) stands for the ability of an individual node to control the communication flow in the networks (Anthonisse 1971; Freeman 1977). Formally, for a node  $v$ , it denotes the total portion of the shortest paths between every pair of

nodes in the network that pass through  $v$  (see more details in Section 3.4). In recent years, betweenness was extensively applied for the analysis of various complex networks (Barthélemy 2004; Strogatz 2001) including, among others, social networks (Scott 2000; Wasserman and Faust 1994), computer communication networks (Faloutsos et al. 1999; Yook et al. 2002), and protein interaction networks (Bork et al. 2004). Holme (2003) has shown that betweenness is highly correlated with congestion in particle hopping systems. Extensions of the original definition of BC are applicable for directed and weighted networks (Brandes 2008; White and Borgatti 1994) as well as for multilayer networks where the underlying infrastructure and the origin–destination (OD) overlay are explicitly defined (Puzis et al. 2007c).

In this work, we discuss the applicability of BC and certain augmented types of it for the prediction of mobility patterns in transportation networks and subsequent deployment optimization of monitoring units in the network. Specifically, we show that there is a strong positive correlation between the traffic that flows through a node in a transportation network and its BC measures. This in turn directly implies a positive correlation between a solution to the betweenness optimization problem and the “collaborative monitoring units deployment problem.” In other words, this duality means that deployment schemes that obtain high betweenness value are also guaranteed to better approximate the maximal monitoring probability deployment.

We define an optimization problem where the cost of deploying a set of monitoring units depends on the properties of routes and intersections they are deployed on (e.g., load, number of lanes, length). In contrast to the cost, effectiveness of monitoring units’ deployment can be measured as the net number of suspected agents (e.g., cars, trucks, etc.) that have been inspected. We show that given a characterization of a potential attack (viz., the weighted graph that represents possible transportation measures the attacking agents may use), we can provide an efficient deployment scheme for the locations of monitoring units. Furthermore, we can also estimate the percentage of traffic this deployment would achieve. These two numbers, put together and combined with the overall cost of a potential attack, yield a “rationality criterion” for investments in monitoring infrastructures, namely, measure of the benefit of the system compared to the expected damage it prevents (see Eqs. 3.4 and 3.6).

The rest of the chapter is organized as follows: Section 3.2 contains an overview of the related work in regards to homeland security and transportation. Section 3.3 describes the transportation dataset that was used in this study. Section 3.4 contains a technical discussion concerning the correlation between BC and traffic flow. Our proposed approach for generating efficient deployment schemes is discussed in Section 3.5, containing first a theoretical basis, followed by a thorough empirical validation using our real-world transportation network dataset—a comprehensive transportation network of the Israeli roads and highways system—containing over 15,000 directed links. Two heuristic methods are presented, and their performance in terms of solution efficiency and computation time is discussed. A short discussion regarding the implications of our proposed method is presented in Section 3.6. A case study of various attack scenarios using the Israeli transportation network is discussed in Section 3.7 and concluding remarks appear in Section 3.8.

### 3.2 RELATED WORK

Homeland security has become one of the dominant aspects with respect to Intelligent Transportation Research since September 11. The importance of *Transportation Systems and Technology* with respect to homeland security and counterterrorism is discussed in details in the official publications of the US National Research Council (Committee on Science and Technology for Countering Terrorism and US National Research Council 2002; The White House 2007). A survey of the homeland security threats and risks regarding transportation infrastructure can be found in Chen et al. (2004).

For example, infectious disease outbreaks pose a critical threat to public health and national security (Berndt et al. 2003; Damianos et al. 2002). Utilizing today's expanded trade and travel, infectious agents can be distributed easily within and across country borders as part of a biological terror attack, resulting in potentially significant loss of life, major economic crises, and political instability. Such threats stress even more the importance of a reliable and efficient transportation monitoring infrastructure. An example for mitigating this risk can be found in Marshall et al. (2004), where an attempt to create a "smart" and safer border is made.

With respect to land transportation, the main focus thus far had been on monitoring the transportation of hazardous materials. It is important to note that the vast majority of works on these topics did not focus on the security-oriented threats (such as preventing terrorists from hijacking these materials and using them in weapons) but, rather, on efficient routing. Efficient routing of hazardous vehicles transportation involves determining what paths vehicles should take to minimize population exposure in the event of an accident. As pointed out in Wright et al. (2006), many authors have developed algorithms and heuristics for solving various cases of the routing problem (Batta and Chiu 1988; Berman et al. 2000; Beroggi and Wallace 1995; Erkut and Ingolfsson 2000; Zografos and Androutsopoulos 2004). In addition, there exist a multitude of works that concern the problem of treating and analyzing the risk that stems from conveying hazardous materials using the national transportation infrastructure (Erkut and Ingolfsson 2005; Kara et al. 2003; Raj and Pritchard 2000).

This work is the first attempt to address this issue from a different angle—trying to predict the traffic patterns of network users of an existing (and optionally dynamic) transportation infrastructure and finding an approximation for the optimal deployment of monitoring units for it. In this sense, this work somewhat resembles the line of work that deals with risk assessment, albeit it is also accompanied with constructive recommendations for policy-makers regarding the appropriate positions (and quantities) of monitoring units that are deployed in order to cope with this risk.

### 3.3 TRANSPORTATION NETWORK DATASET

The widespread use of cellular phones in Israel enables the collection of accurate transportation data. Given the small size of the country, all cellular companies provide national-wide coverage. As shown in Bekhor et al. (2013), the penetration of cellular phones to the Israeli market is very high, even to lower-income households

and specially among individuals in the ages of 10–70 (the main focus of travel behavior studies). Such penetration enables a comprehensive study of travel behavior that is based on the mobility patterns of randomly selected mobile phones in the Israeli transportation system. This data was shown in Bekhor et al. (2013) and Gur et al. (2009) to provide a high-quality coverage of the network, tracking 94 % of the trips (defined as at least 2 km in urban areas and at least 10 km in rural areas). The resulting data contained a wealth of traffic properties for a network of over 6000 nodes and 15,000 directed links. In addition, the network was accompanied with an OD matrix, specifying start and end points of trips.

The network was created for the National Israeli Transportation Planning Model. In urban areas, the network contains arterial streets that connect the interurban roads. For each link of the network, there is information about the length (km), hierarchical type, free-flow travel time (min), capacity (vehicles per hour), toll (min), hourly flow (vehicles per hour), and congested travel time (min). The hourly flows and congested travel times were obtained from a traffic assignment model that loads the OD matrix on the network links.

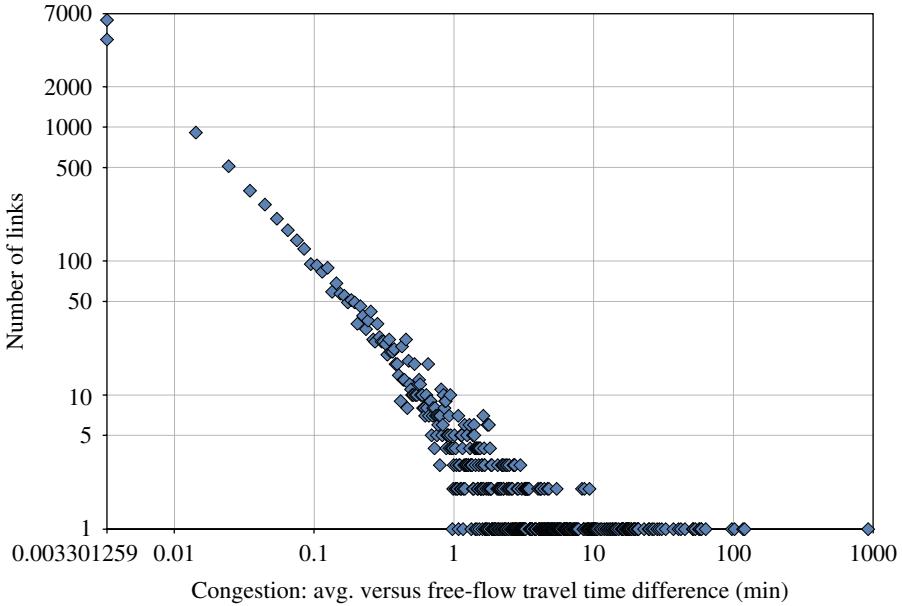
### 3.3.1 Network Structure

Based on the dataset described previously, we have created a network structure, assigning running indices from 1 to 6716 to the nodes (junctions). We have examined the directed variant of the network where each road segment between two junctions was represented as either one or two directed links between the respective nodes.

In order to get a basic understanding of the network, we first extracted and studied several of its structural properties (see Table 3.1). We have partitioned the network into structural equivalence classes of the nodes and biconnected components and computed the BC indices of the nodes (Freeman 1977; Lerner 2005; Lorrain and White 1971). Structurally equivalent vertices have exactly the same neighbors, and the set of these vertices is called a structural equivalence class. As can be seen from Table 3.1, the number of structural equivalence classes is roughly the number of vertices in the network, and the size of the largest class is three. This means that there are no “starlike” structures in the network and alternative paths between any two vertices are either longer than two hops or have other links emanating from the intermediate vertices. On the other hand, the number of biconnected components in the network is low compared to the number of nodes, meaning that there are significant regions of the network that can be cut out by merely disconnecting a single node.

**TABLE 3.1 Structural Properties (Israeli Transportation Network)**

Nodes	6,716
Edges (undirected representation)	8,374
Edges (directed representation)	15,823
Number of structural equivalence classes	6,655
Largest equivalence class	3
Number of biconnected components (BCC)	931
Average BCC size	8.2
Largest BCC	5,778



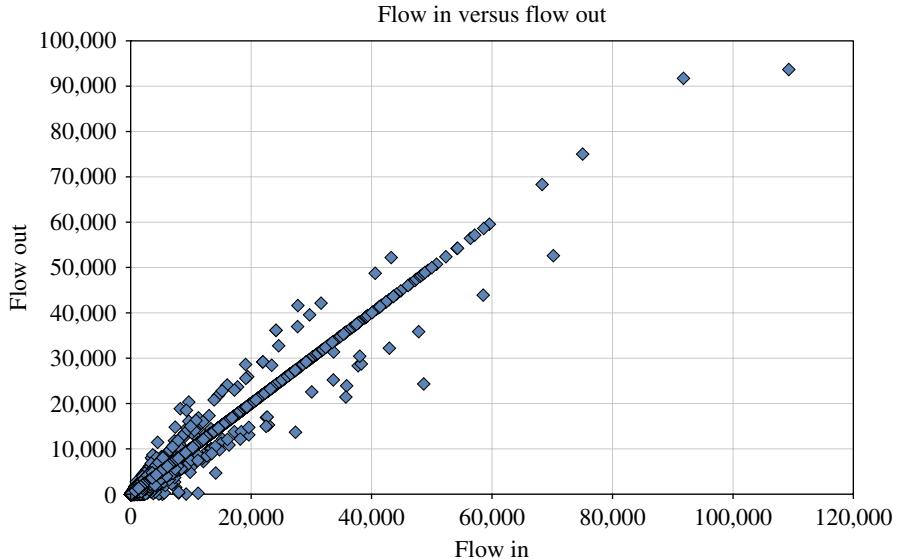
**FIGURE 3.1** Power law distribution of congestion.

### 3.3.2 Congestions

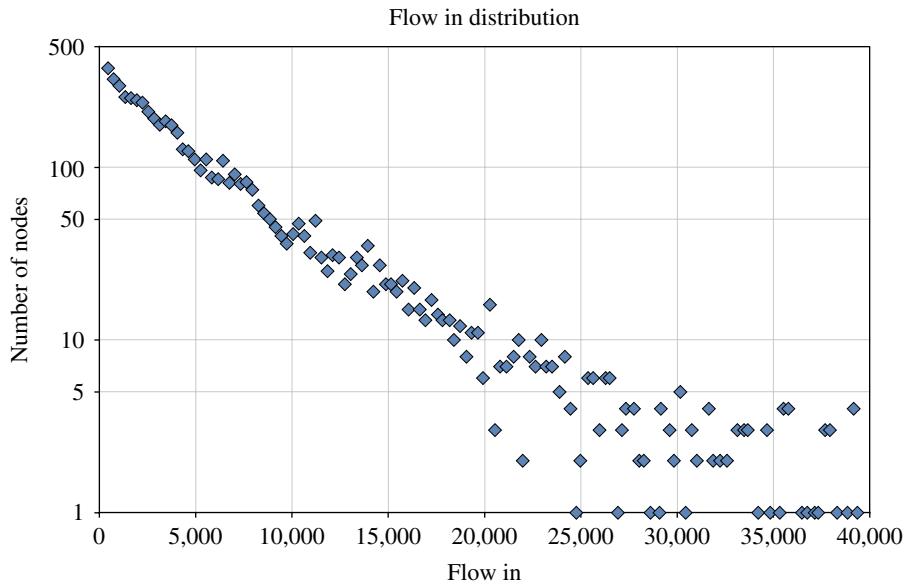
In this chapter, we define the impact of congestion as the difference between the time to travel through a congested link and the free-flow time to travel. Congestion of a junction can be either inbound or outbound. Inbound congestion is the sum of all congestions on inbound links of some junction. Figure 3.1 presents the distribution of congestion on network nodes (junctions). Power law nature of this distribution means that vast the majority of nodes are not congested, but there are a few nodes whose congestion can be arbitrarily large. Based on *Wardrop's user equilibrium* (Wardrop 1952), this also implies a low number of yet significant deviations between the routes chosen by travelers during free flow and during congestions. In Section 3.4.3, we use this fact to merge between two routing strategies.

### 3.3.3 Flow

The analyzed dataset contains traffic flow through links provided as the number of vehicles per hour. In the next section, we will compare the flow through nodes estimated using BC to the measured flow. We compute the total inbound flow through a node by summing flows on all of its inbound links, where outbound flow is computed symmetrically. Unless a specific junction is a source or a destination of traffic, we expect the inbound flow to be equal to the outbound flow. Figure 3.2 demonstrates the correlation between inbound and outbound flow. We see that vast majority of the nodes are located on the main diagonal; however, there are some deviations caused by the fact that the data represents average measurements that were carried out along a substantial period of time.



**FIGURE 3.2** Incoming versus outgoing flow for each node.



**FIGURE 3.3** Exponential distribution of traffic flow through nodes.

Figure 3.3 presents the distribution of inbound flow on network nodes. This distribution is exponential, meaning that a vast majority of nodes have little flow through them. However, in contrast to network congestion, there are no “unbounded fluctuations,” that is, the flow through the most “busy” junctions is not as high as can

be expected from the power law distribution of betweenness and congestions (Figs. 3.1 and 3.4). In fact, congestions significantly limit the flow through the busiest junctions, which subsequently is the reason we do not see the long tail in flow distribution.

### 3.4 BC VERSUS TRAFFIC FLOW

BC is defined as the total fraction of the shortest paths between each pair of vertices that pass through a given vertex (Freeman 1977). Let  $G = (V, E)$  be a directed transportation network where  $V$  is the set of junctions and  $E$  is the set of directed links as described in Section 3.3. Let  $\sigma_{s,t}$  be the number of the shortest paths between the origin vertex  $s \in V$  and the destination vertex  $t \in V$  (in some applications, the shortest path constraint can be relaxed to allow some deviations from the minimal distance between the two vertices). In the rest of this chapter, we will refer to the shortest or “almost” shortest paths between two vertices as *routes*. Let  $\sigma_{s,t}(v)$  be the number of routes from  $s$  to  $t$  that pass through the vertex  $v$ . The BC can hence be expressed by the following equation:

$$\text{BC}(v) = \sum_{s,t \in V} \frac{\sigma_{s,t}(v)}{\sigma_{s,t}} \quad (3.1)$$

Note that in this definition, we include the end vertices ( $s$  and  $t$ ) in the computation of betweenness since we assume that vehicles can be inspected also at their origin and at the point of their destination.

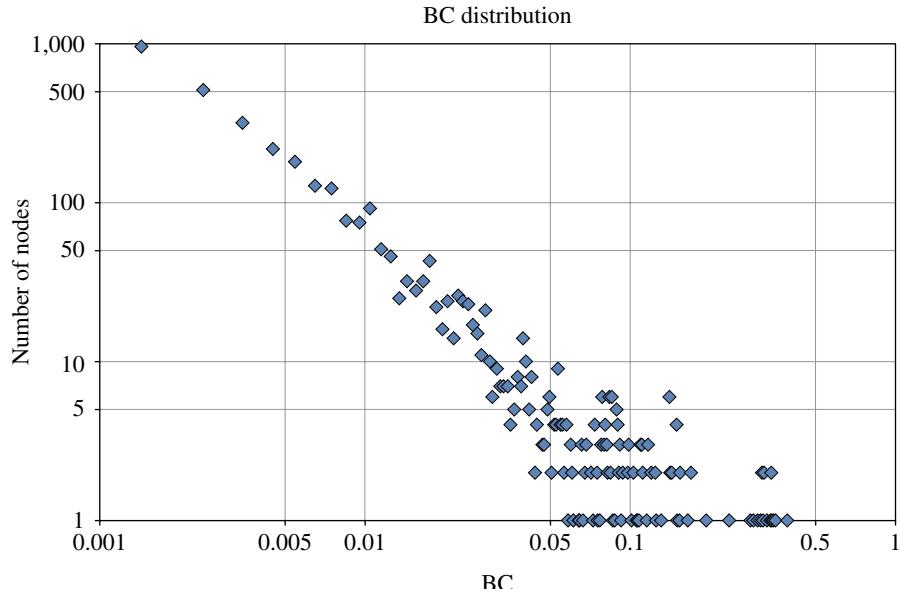
After computing the BC for the given transportation network, we can easily see that the distribution of BC follows a power law (Fig. 3.4). Long-tail distributions such as the power law suggest that there is a nonnegligible probability for existence of vertices whose BC can be arbitrarily high. This is in contrast to the exponential flow distribution depicted in Figure 3.3. The different nature of these two distributions suggests that BC as defined previously will overestimate the actual traffic flow through nodes especially for the most central vertices.

Next, we would like to check the correlation between BC and traffic flow. Although the correlation is significant, the square error is very low ( $R^2 = 0.2021$ ) as shown in Figure 3.5a. Every point in this figure represents a vertex with the  $x$ -axis corresponding to the measured traffic flow and  $y$ -axis corresponding to the computed BC.

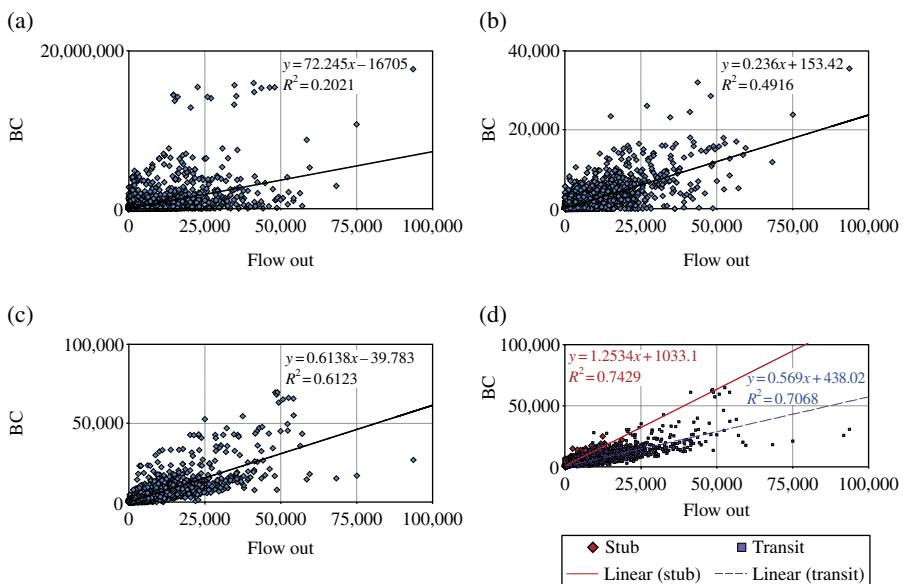
We now discuss augmented variants of the BC measure that significantly improve the correlation with the traffic flow.

#### 3.4.1 OD-Based BC

According to Equation 3.1, BC assumes equal weights of routes between every pair of vertices in the network. In other words, every vertex acts as an origin and as a destination of traffic. We would like to utilize the measured OD flow matrix in order



**FIGURE 3.4** Power law distribution of betweenness centrality.



**FIGURE 3.5** Correlation of flow through nodes and betweenness centrality showing a consistent positive correlation between increase in the betweenness centrality and the outgoing flow. (a) BC classical definition. (b) BC w.r.t. OD matrix. (c) BC w.r.t. OD matrix and free-flow travel time. (d) BC w.r.t. OD matrix, free-flow, and congested travel time.

to prioritize network regions by their actual use. For this, we shall use the following altered definition for betweenness, as suggested in Puzis et al. (2007c):

$$\text{BC}(v) = \sum_{s,t \in V} \frac{\sigma_{s,t}(v)}{\sigma_{s,t}} \times \text{OD}_{s,t} \quad (3.2)$$

where OD is the actual measured OD matrix. This method produces a better correlation ( $R^2 = 0.4916$ ) between the theoretic (BC) and the measured traffic flow (see Fig. 3.5b).

### 3.4.2 Shortest Routes Based on Time to Travel

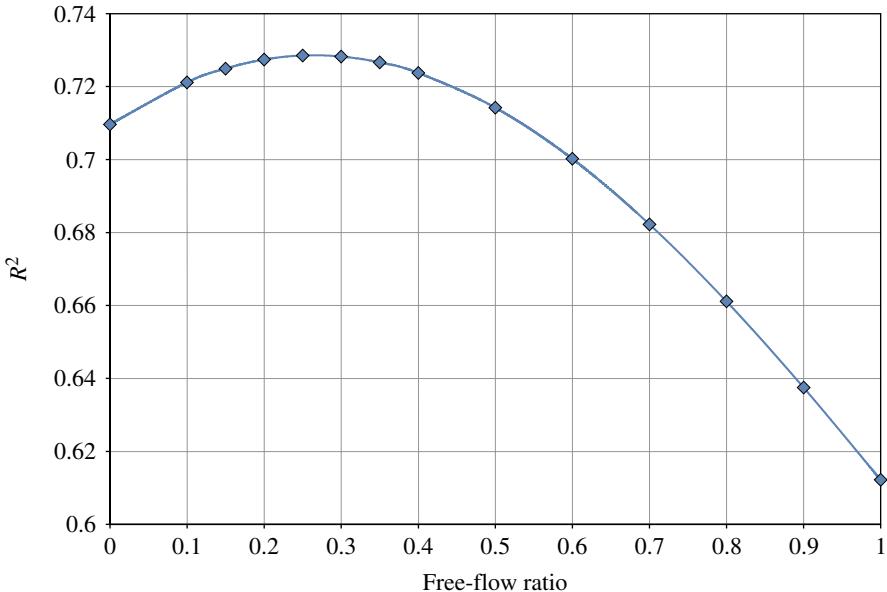
In order to further improve our ability to estimate the predicted network flow using the network's topology, we note that both BC calculation methods (Eqs. 3.1 and 3.2) assume that routes are chosen according to the shortest path strategy based on hop counting. In this section, we retain the shortest path assumption but use weighted links for calculating the betweenness score. One option is to use the length of the road segments as their weights for the shortest path calculations (based on the well-justified assumption that people prefer short routes over the long ones). However, the road capacity, congestions, and the number of segments also play significant roles when choosing the route to destination. People would prefer highways over sideways when the distance difference is not high.

The shortest path algorithms (such as Dijkstra's or Bellman–Ford's) are able to consider only one distance weight on links when computing the shortest path to a destination. We shall therefore assume that the primary heuristic guiding people when they chose a route is the time required to reach their destination. Using this assumption, we recompute the BC on the directed transportation, weighting links by their free-flow travel time.

Let  $\text{BC}^{\text{ff}}(v)$  denote the betweenness of a node  $v$  computed w.r.t. the free-flow travel time. Figure 3.5c shows significant improvements in the correlation between the measured traffic flow and the theoretical  $\text{BC}^{\text{ff}}$  values computed w.r.t. the OD matrix and free-flow travel time link weights ( $R^2 = 0.6123$ ). We can see that there are few nodes whose flow was significantly underestimated by the BC measure. Notice that there are also several nodes whose flow was actually overestimated. This can be explained by the fact that people do not travel strictly via the shortest paths, but may have various deviations. In particular, the deviations from the shortest paths are affected by the day time and the day of the week.

### 3.4.3 Peak Hour-Aware BC

It is a reasonable assumption that during peak hours, travelers will choose to avoid the congested roads and choose their routes based on the congested travel time rather than on the free-flow travel times. Let  $\text{BC}^{\text{ct}}(v)$  denote the betweenness of a node  $v$  computed w.r.t. the congested time. Computing betweenness using only the congested



**FIGURE 3.6** Squared error ( $R^2$ ) as the function of the free-flow traffic fraction ( $\alpha$ ).

travel time weights results in  $R^2 = 0.7096$ . Although peak hours are relatively small fraction of the day, most vehicles travel at these hours. This is the reason for higher correlation of  $BC^{ct}$  with the measured traffic flow.

We shall now combine both the BC computed w.r.t. the free-flow travel time and the congested time by taking a weighted average, namely,

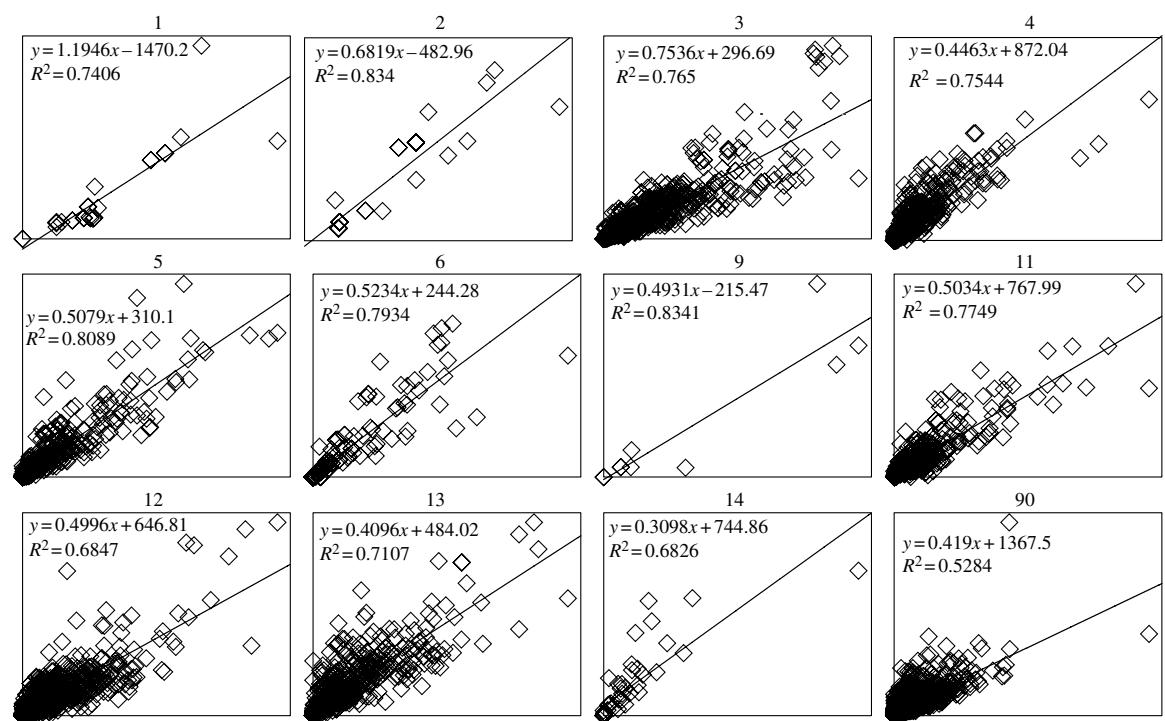
$$BC(v) = \alpha \times BC^{ft}(v) + (1 - \alpha) \times BC^{ct}(v)$$

where  $\alpha$  denotes the relative fraction of vehicles traveling during the free-flow periods. The resulting centrality index can achieve higher correlation with the measured average traffic flow. The maximal correlation of  $R^2 = 0.7285$  is obtained for  $\alpha = 0.25$  as shown in the Figure 3.6.

### 3.4.4 Separating Stub Nodes from Transit Nodes

Carefully looking at the various nodes, we can see that they can be divided into two groups: *stub nodes* and *transit nodes*.

A stub node is a node that is an origin or a destination of the traffic (as seen in the OD matrix). These nodes account for approximately 10% of the network's nodes. All other nodes (viz., nodes that generate insignificant or no outgoing or incoming routes) are called transit nodes, as they only forward traffic and do not generate or consume it.



**FIGURE 3.7** Correlation of flow through nodes and betweenness computed separately for different *types* of links.

Figure 3.5d presents the correlation that is received when the two groups of nodes are being processed separately. Specifically, the results show a  $R^2 = 0.7068$  for the transit nodes and a  $R^2 = 0.7429$  for the stub nodes.

### 3.4.5 Mobility-Oriented BC

As previously mentioned, the transportation network dataset we use contains a “*type*” attribute for each link, representing the domain-specific “*role*” of the link in the overall network. For example, links of types 13 and 14 correspond to internal neighborhood roads, whereas links of type 12 correspond to “collectors”—roads that are in charge of aggregating the traffic from neighborhood roads and channeling it to metropolitan roads and so on. As each type of roads have therefore a different role, we now try to further improve our flow prediction by examining the betweenness values achieved when calculating it for every group separately.

The results of the correlation that is achieved using this method are presented in Figure 3.7. We can clearly see that for the more important roads (viz., those with a lower-type number, representing a more infrastructural role in the transportation network), this technique yields  $R^2$  values that are consistently above 0.74, reaching 0.83(!) for road of types 2 and 9 (note that roads of type 90 are fictive roads with infinite capacity that were artificially added in order to connect distinct regions in the network).

It should be noted that each node may have incoming roads of different types. Each plot corresponds to a set of nodes whose max incoming road type is as specified. In addition, the BC calculations were not made for each set of nodes separately—BC was computed for the complete network, while the correlations were computed separately for each type.

## 3.5 OPTIMIZING THE LOCATIONS OF SURVEILLANCE AND MONITORING STATIONS

In this section, we use the group variant of the shortest path betweenness centrality (GBC) (Everett and Borgatti 1999) as an estimate for the utility of collaborative monitoring for homeland security threats. In other words, we are interested in verifying that given some mobile threat agent, we position the monitoring stations in a way that maximize the chance the agent would be captured, given the traffic patterns of the transportation network. In this case, however, significant computational complexity issues arise, rendering the generation of an optimal solution impractical in real time by conventional tools that are based mostly on behavioral-based modeling. Using GBC, we propose a way to generate efficient approximations of the optimal solution to this optimization problem.

GBC of a given group ( $M \subseteq V$ ) of vertices accounts for all routes that pass through *at least one* member of the group. Let  $\sigma_{s,t}(M)$  and  $\sigma_{s,t}^*(M)$  be the number of routes from  $s$  to  $t$  and the number of routes from  $s$  to  $t$  passing through at least one vertex in  $M$ , respectively,

$$\text{GBC}(M) = \sum_{s,t \in V} \frac{\sigma_{s,t}(M)}{\sigma_{s,t}(M)} \times \text{OD}_{s,t} \quad (3.3)$$

GBC can be efficiently computed using the algorithm presented in Puzis et al. (2007a).

Assuming the routes are weighted by the OD flow in transportation networks, GBC will account for the net number of vehicles that are expected to pass by the monitors during an hour. This net number is different from the total number of vehicles passing by the monitors since the same vehicle can pass by several monitors during a single trip. For example, searching for a suspected escaping terrorist car, one would like to avoid stopping the same vehicle twice and increase the number of distinct vehicles that were inspected. It is therefore important to maximize the GBC value of the set of inspection stations given the number of stations deployed.

Several combinatorial optimization techniques can be used to find a group of nodes of given size that has the largest GBC. In the following discussion, we refer to a greedy approximation algorithm for the monitor location optimization problem (*greedy*) (Dolev et al. 2009), a classical *depth first branch and bound* (DFBnB) heuristic search algorithm (Korf and Zhang 1995), and the recently proposed *potential search* (Stern et al. 2011).

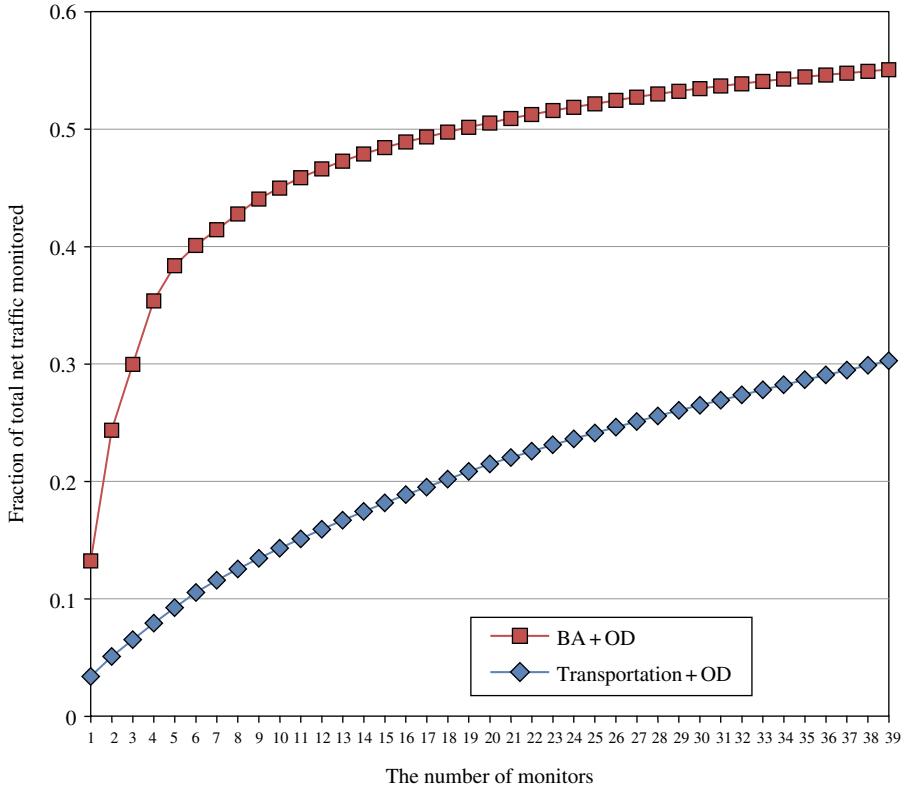
The *greedy* approximation algorithm chooses at every stage the node that has the maximal contribution to the GBC of the already chosen group. The approximation factor of the *greedy* algorithm as reported in Dolev et al. (2009) is

$$e - \frac{1}{e} \approx 0.632$$

Both the heuristic search algorithms *DFBnB* and the *potential search* provably find the group having the maximal GBC. The *greedy* algorithm and *DFBnB* were previously compared in Puzis et al. (2007b) in the context of monitoring optimization in computer communication networks. The authors have shown that in preferential attachment networks (Barabasi and Albert 1999), greedy algorithm produced results that are 0.3% far from optimal. Given the fact that finding a group of a given size having the maximal GBC is a hard problem,<sup>1</sup> the greedy algorithm is good enough for any practical purpose. Figure 3.8 presents the results of selecting 1–39 inspection locations using the greedy algorithm.

In homeland security applications, deployment of monitoring systems are often done under tight timing conditions as a result of new intelligence information. Therefore, any optimization method should provide close to real-time capabilities. In this context, it is interesting to note that both the *DFBnB* and

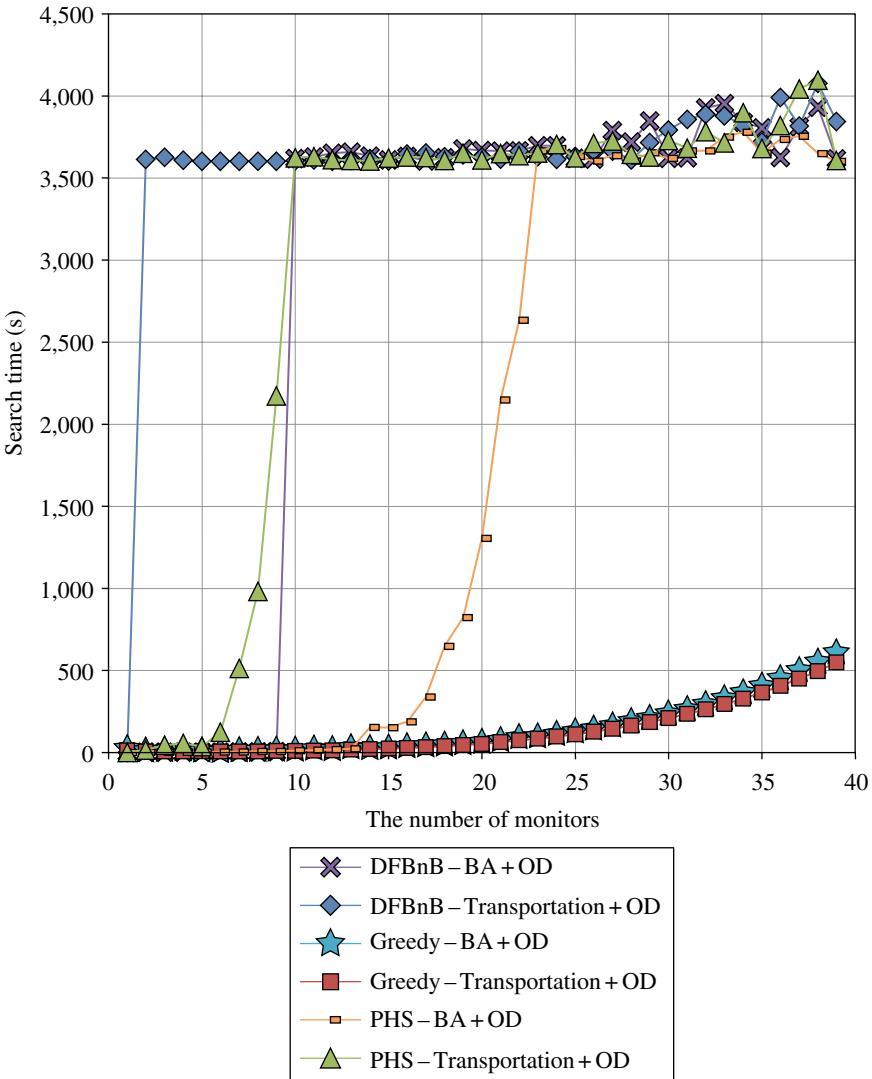
<sup>1</sup>It can be proven by a straightforward reduction from the minimal vertex cover problem that the problem of maximizing GBC is NP complete.



**FIGURE 3.8** The total net traffic flow that passes by monitors as a functions of the number of monitors. As expected, the marginal value of additional monitors gradually decreases as more of them are added, reaching potential traffic coverage of 30% when 39 monitoring stations are deployed.

the *Potential* algorithms are anytime search algorithms (Zilberstein 1996). Their execution can be stopped at any point of time, yielding the best solution found so far. Therefore, in the following experiments, we limit the search time to 1 h, simulating a quasi-real-time optimization constraint. Still, as can be seen in Figure 3.9, the running time of the *greedy* algorithm is by far lower than 1 h for the entire Israeli transportation system.

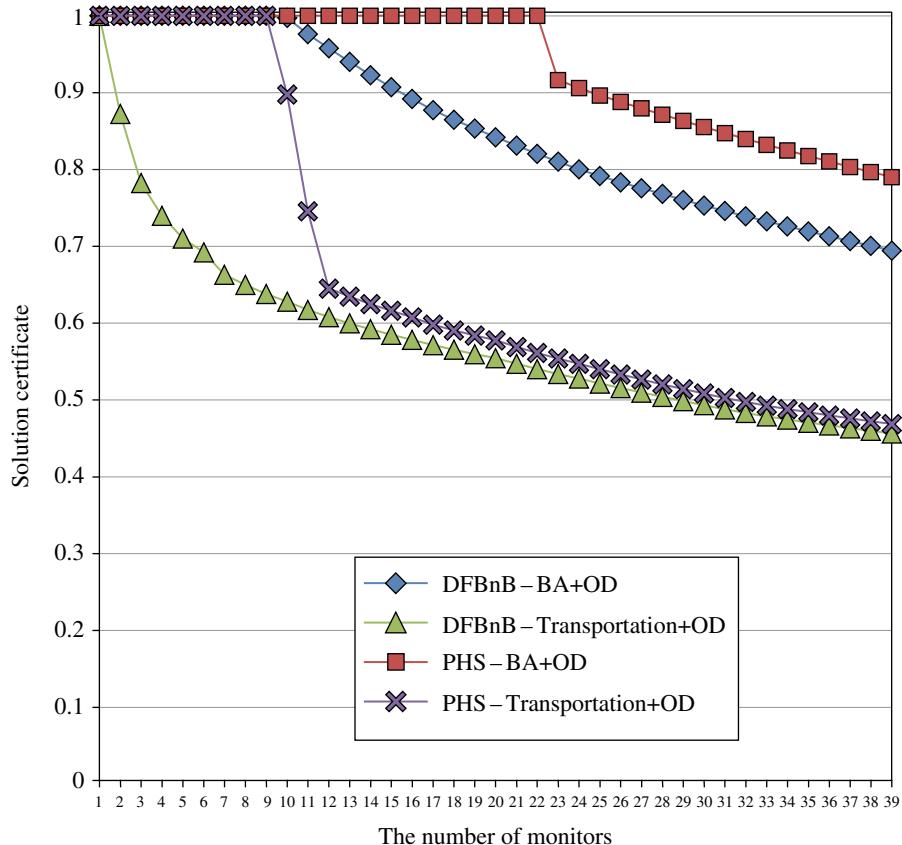
When *DFBnB* and *potential search* algorithms cannot complete the search process within the given time bounds, they produce a close to optimal solution and an estimate of its optimality (i.e., certificate). The certificate is computed by dividing the best solution found so far by the upper bound on the optimal solution. The upper bound is computed using admissible heuristic functions and is maintained by the search algorithms for efficient pruning the search space. Figure 3.10 shows that *potential search* produces higher certificates for its solutions within the one hour time bound for all sizes of the monitor deployment.



**FIGURE 3.9** The time (in seconds) that the search algorithms were executed as a function of the number of monitors.

### 3.6 APPLICATIONS AND CONSIDERATIONS FOR POLICY-MAKERS

As discussed in the introduction of this work, a strong positive correlation can be found between the BC of nodes of a transportation network and the traffic volume that they have access to. Hence, monitoring deployment schemes that are characterized in high betweenness values would be far more likely to successfully intercept potential threats compared to low betweenness ones.



**FIGURE 3.10** The minimal quality of the solution (fraction of the upper bound) as a function of the number of monitors.

This understanding can be used by policy-makers in order to enhance the coverage performance of the existing nation-level infrastructure monitoring system, as well as design protocols for fast response that could be used ad hoc in case of alerts regarding a suspected threat. In such cases, the two most dominant factors are response time and overall monitoring probability (the probability that the target, if such exists, would eventually be engaged). Hence, as response time is usually predefined and is heavily affected by many other factors, having the ability to improve the monitoring factor, for any short response time, is of the utmost importance. Moreover, using our proposed method implies that monitors can be deployed/activated gradually as they are needed (due to operational requirements or budget constraints).

In addition, we should note that it is not necessary to know ahead of time the total number of monitors that will be deployed in order to find their optimal locations. Upon requirement of additional monitors units, their locations can be suggested

based on up-to-date network data as well as the current deployment (the effectiveness of this method is very close to optimal both in communication and transportation networks).

Another interesting issue to be considered is the trade-off between the number of monitoring units and their quality with respect to the number of vehicles each unit can monitor simultaneously (to be denoted as the units' "*sampling rate*," ranging between 0 and 1). Note that higher sampling rates directly imply a higher cost per unit. Therefore, the overall cost of the monitoring system can be modeled as

$$\text{Overall cost} = \text{cost per unit} \times \text{number of units}$$

whereas the overall monitoring performance of the system can be modeled as

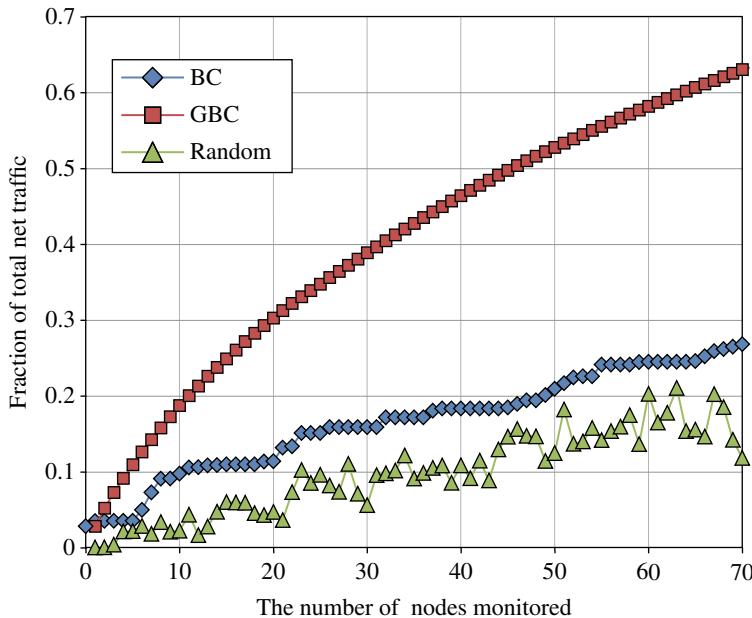
$$\begin{aligned}\text{Overall performance} &= \text{system monitoring prediction} \times \text{sampling rate} \\ &= f_{BC}(\text{number of units}) \times f_{\text{sampling}}(\text{cost per unit})\end{aligned}$$

For a given budget, the decision whether to deploy a higher number of units or to invest to units of better monitoring capabilities can be directly resolved by studying the functions  $f_{BC}$  and  $f_{\text{sampling}}$ . Whereas the first was thoroughly studied in the previous sections, analyzing the effect of the sampling rate over the performance of the system is a much simpler task (Dolev et al. 2010). With low sampling rates, GBC becomes proportional to the sum of BC values of the group members (as the number of redundant inspections reduces with the sampling rate). We can, therefore, consider a guideline saying that traffic monitors with very low sampling rates can be deployed on the most central nodes in the network, even if it means deploying several monitors on the same node. However, when the overall sampling rate of monitors deployed on each node is relatively high, then the set of monitored nodes should be chosen wisely using a more rigorous execution of the optimization algorithm.

Notice that BC- and GBC-based deployments have the same utility when selecting a single monitor as expected. However, GBC-based strategy continuously improves the traffic coverage as more monitors are added with the marginal utility of each additional monitor slowly decreasing.

Figure 3.11 demonstrates the performance of our monitoring method, by showing the percentage of traffic monitored as a function of the number of monitors, for several deployment schemes: (i) group betweenness, (ii) betweenness, and (iii) random deployment. The benefits of the proposed method can clearly be seen from this chart.

BC-based strategy produces relatively high-quality deployments for a small number of monitors (<5). However, when 10 or more monitors need to be located, random deployment is on average as effective as choosing the most central intersections. Moreover, for large numbers of monitors (>70–80), random deployment, although the simplest strategy, achieves coverage results that are very similar to choosing the most central intersections. This result may seem surprising but in fact it is absolutely reasonable. Central intersections tend to lay on the arterial roads and



**FIGURE 3.11** The figure presents the results of deployment optimization performed on the Israeli transportation network with average travel times computed using state-of-the-art traffic assignment model. The flows and the utility of the deployment were estimated using *betweenness centrality* (BC) and *group betweenness centrality* (GBC) models and compared also to the random deployment model. Whereas the BC algorithm had chosen the locations for monitoring units according to the most central intersection based on their BC values, the GBC deployment was a greedy algorithm that tried to maximize the net number of vehicles passing by the monitors. The benefits of the GBC strategy are clearly shown, as well as the ability to extrapolate this correlation between the number of monitoring units and monitored traffic percentage, in order to find the minimal number of monitoring units required in order to guarantee certain levels of coverage.

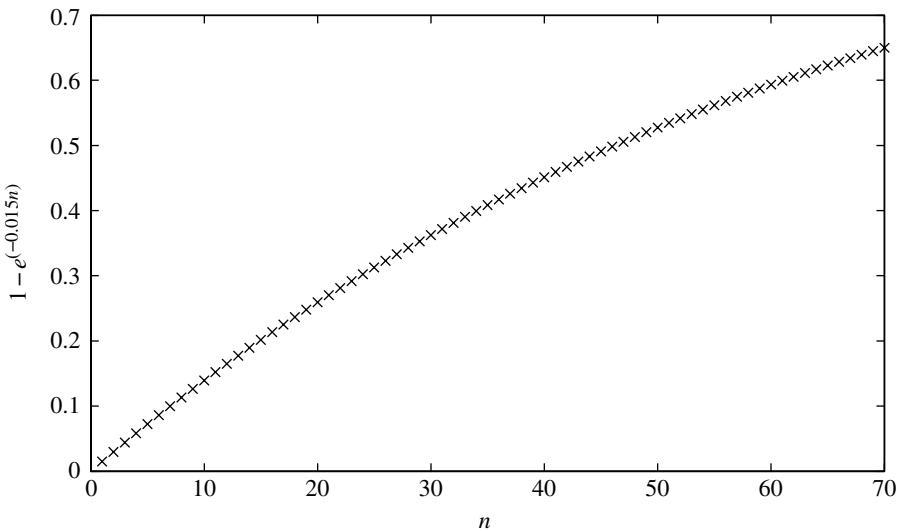
usually are quite close to each other. This results in reduced marginal utility of each additional junction joining the deployment.

Using the results of Figure 3.11, the effect of the number of monitors over the overall percentage of traffic coverage can be observed and used by policy-makers in order to decide on the optimal monitoring strategy.

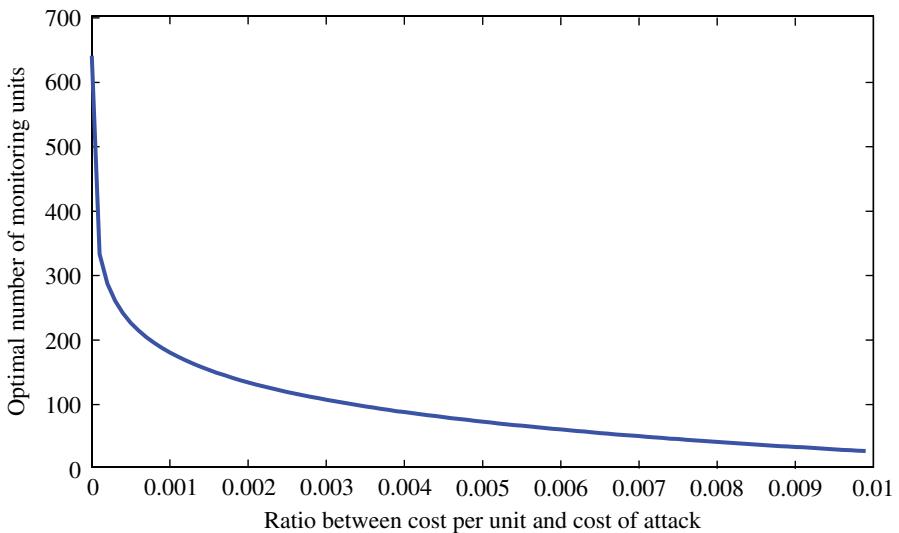
**Definition 3.1:** Let us denote the cost of an attack as  $\varphi_{\text{attack}}$ .

**Definition 3.2:** Let  $M(x): \mathbb{Z}^+ \rightarrow [0,1]$  be a monotonous function denoting the percentage of traffic that is monitored using  $x$  monitoring units.<sup>2</sup>

<sup>2</sup>The function  $M(x)$  can be extrapolated using simulations, as demonstrated in Figure 3.11. Note that  $M(x)$  is domain dependent and may significantly change for different networks.



**FIGURE 3.12** An illustration of the function  $M(n) = 1 - e^{-0.015n}$  that may be used as a model of the simulative results that are presented in Figure 3.11.



**FIGURE 3.13** The optimal number of monitoring units as a function of the ratio between the cost of a single monitoring unit and the cost of a successful attack (assuming the regression of the traffic coverage function to the function  $M(n) = 1 - e^{-0.015n}$ ).

Therefore, an investment in a monitoring system of  $n$  units would be a rational decision as long as

$$\wp_{\text{attack}} \geq \frac{n}{M(n)} \times \text{cost per unit} \quad (3.4)$$

If we focus on the monetary costs of attacks and disregard other aspects, then we see that the *normalized benefit* of a monitoring system can be defined as

$$\omega \triangleq \wp_{\text{attack}} \times M(n) - n \times \text{cost per unit} \quad (3.5)$$

The optimal value of the normalized benefit would then be received for the number of monitoring units that nulls the derivative  $\partial\omega/\partial n$ :

$$\frac{\partial\omega}{\partial n} = \wp_{\text{attack}} \times \frac{\partial M(n)}{\partial n} - \text{cost per unit}$$

Namely,

$$\frac{\partial M(n)}{\partial n} = \frac{\text{cost per unit}}{\wp_{\text{attack}}} \quad (3.6)$$

For example, if we use the function  $y = 1 - e^{-0.015x}$  in order to model the function  $M(n)$  (see Fig. 3.12), after assigning it to Equation 3.6, we will obtain

$$0.015 \times e^{-0.015n} = \frac{\text{cost per unit}}{\wp_{\text{attack}}}$$

which in turn implies

$$n = \frac{\ln(0.015 - \ln(\text{cost per unit}/\wp_{\text{attack}}))}{0.015} \quad (3.7)$$

This is demonstrated in Figure 3.13, where the optimal number of monitoring units is presented, for any ratio between the cost of a single monitoring unit and the expected cost of a successful attack, based on the regression to the function that is presented in Figure 3.12.

### 3.7 CASE STUDY: ATTACK SCENARIOS IN THE ISRAELI NETWORK

In this section, we examine the normalized benefit estimation of various monitoring systems, for several attack scenarios, using the Israeli transportation network. We use the function  $y = 1 - e^{-0.015x}$  in order to approximate the evolution of our monitoring

coverage with the increase in monitoring units, as illustrated in Figure 3.12. We use Equation 3.7 in order to calculate the optimal number of monitoring units and Equation 3.5 in order to estimate the normalized benefit of the monitoring system.

### 3.7.1 Scenario I (Limited Threat)

A truck filled with oil gets overturned on a highway. The oil needs to be cleaned, but it does not spread and is not lethal when exposed to. The main damage is the delay caused to the cars that get stuck in the huge traffic jam. Fast detection of the accident can save \$500,000 in wasted work hours.

### 3.7.2 Scenario II (Local Threat)

A criminal prisoner escapes from prison and evades the police for hours, using a stolen car with known license plate number. A stationary traffic monitoring camera eventually tracks him down, not before he was able to rob a liqueur store, severely injuring the clerk and three customers. Costs of the chase and compensations to the victims are \$5,000,000.

### 3.7.3 Scenario III (Metropolitan Threat)

A car packed with C4 plastic explosive and propane tanks, driven by a suicide bomber, rams the basis of an interchange carrying three levels of freeway as well as the main line of the metro rail. In the collapse of the interchange, 20 are killed and the train traffic in the metropolitan area suffers disruptions for 2 months, while the trains are rerouted to alternative rails until the damage is fixed. Costs are estimated in \$50,000,000.

### 3.7.4 Scenario IV (Regional Threat)

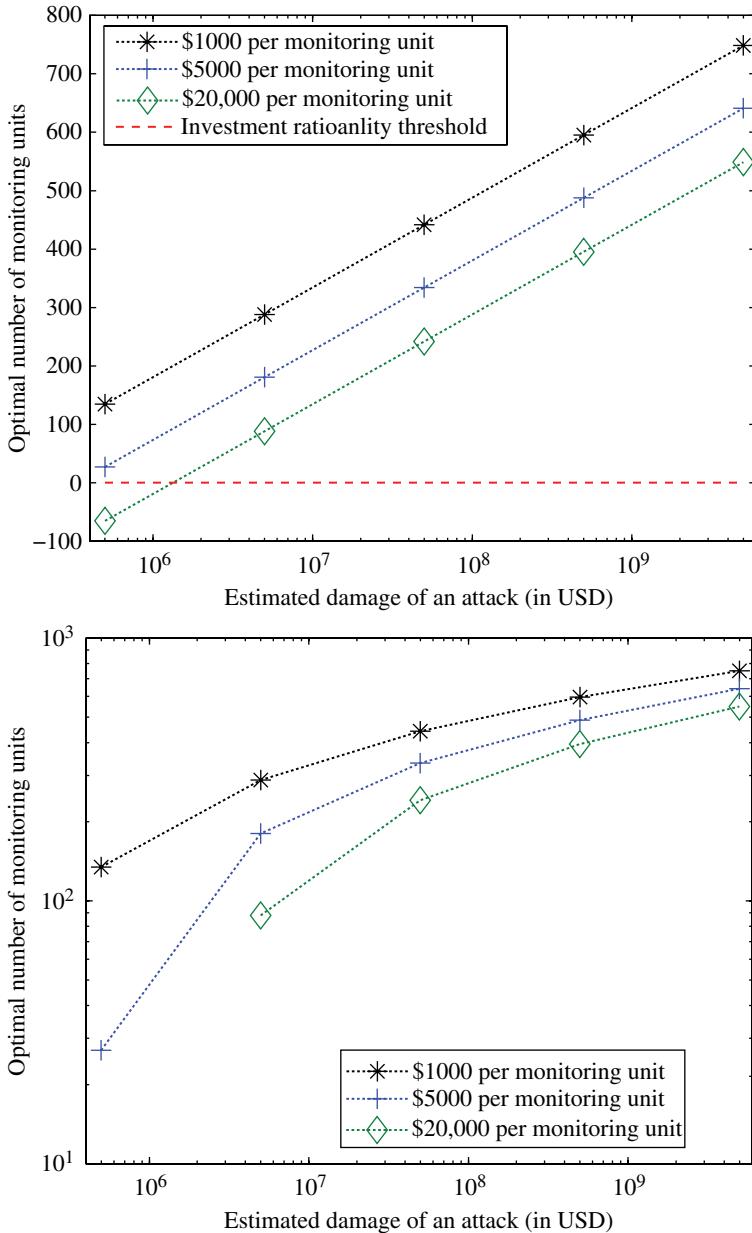
A trailer carrying toxic liquid waste leaks due to bad maintenance while driving through the interstate. Thirty miles of the road needs to be closed for 2 weeks while the road is cleaned. Total damage soars to \$500,000,000.

### 3.7.5 Scenario V (National Threat)

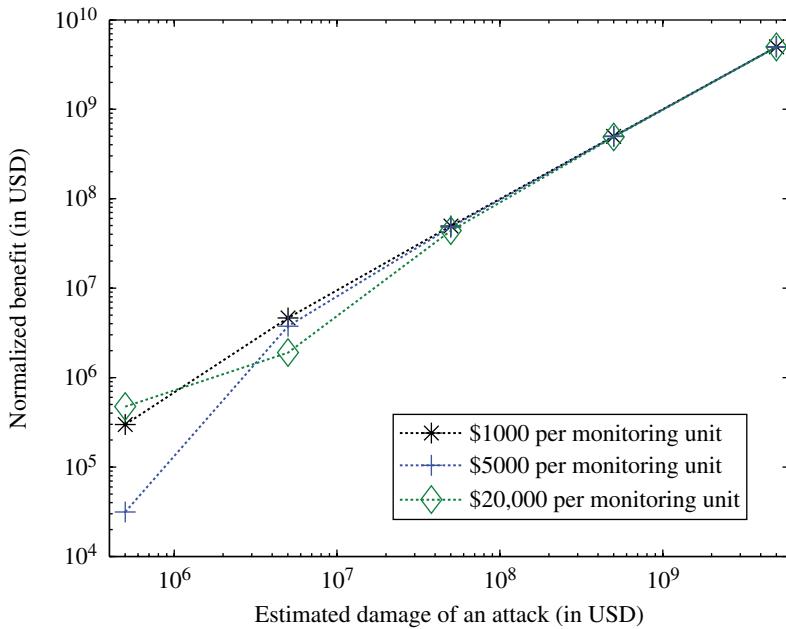
A van carrying a “dirty bomb” gets smuggled into the main street and detonated. There are eight thousand causalities, and radioactive pollution makes the major part of the city center uninhabitable. Total damage reaches \$5,000,000,000.

We examine three different kinds of monitoring units, ranging from \$1000 through \$5000 to \$20,000 (e.g., the cost of a small-scale stationary unit equipped with low-bandwidth communication channel and sensors that can detect chemical or radioactive agents).

Figure 3.14 depicts the optimal number of monitoring units for these five attack scenarios for the three different types of monitoring units. Notice how the optimal



**FIGURE 3.14** The optimal number of monitoring units for three different types of units, ranging from \$1000 through \$5000 to \$20,000 in price, using the normalized benefit model. The charts illustrate the results of the model for five different attack scenarios of \$500,000, \$5,000,000, \$50,000,000, \$500,000,000, and \$5,000,000,000 in total damages. Notice that both charts are in log scale in the X-axes. However, the top chart depicts the results in linear scale, whereas the bottom charts uses a double-log scale. The horizontal dashed line on the upper chart represents the *investment rationality threshold*, below which the normalized benefit on investing in a monitoring system would be negative. This chart assumes that the increase in monitoring coverage as a function of the number of monitoring units can be approximated using the function  $M(n) = 1 - e^{0.015n}$ .



**FIGURE 3.15** The *normalized benefit* of the monitoring system using the GBC method for three different types of units, ranging from \$1000 through \$5000 to \$20,000 in price. The chart illustrates the results of the model for five different attack scenarios of \$500,000, \$5,000,000, \$50,000,000, \$500,000,000, and \$5,000,000,000 in total damages.

number of units is linearly increased as the damage costs are increased in orders of magnitude. Namely, due to the high monitoring efficiency obtained using the proposed GBC method, a relatively low number of units would be ideal for almost any kind of attack scenarios.

Figure 3.15 demonstrates the normalized benefit of the system. Notice that due to the extremely high efficiency of the proposed GBC-based monitoring method, the normalized benefit of the system can be made very close to the cost of the attack. That is, the normalized cost of the system is close to zero.

### 3.8 CONCLUSIONS

In this chapter, we have discussed the problem of optimizing the locations of surveillance and monitoring stations for a variety of homeland security purposes. For this problem, known to be of high complexity, we propose a novel approximation using the quasi-real-time calculation of the BC of the network. For this, we show a correlation between the BC of a node and its expected traffic flow in transportation networks. Using a comprehensive dataset that covers the Israeli transportation network, we have

first performed a simple analysis of the network and its properties, showing that there exists a correlation between the traffic flow of nodes and their BC. We then revised the basic definition of BC, showing that when analyzing the network in a way that takes into account additional known properties of the links (specifically time to travel through links), a much stronger correlation can be achieved. Taking into account that a large portion of the traffic is being generated during rush hours and that different roads may have different “roles” in the transportation network, we show that a significantly higher correlation can be achieved when clustering the roads into groups based on their types (a known property of each road) while also giving increased weight to data that is associated with certain hours. Using this method that we call “mobility-oriented BC,” we demonstrate correlation values of approximately  $R^2 = 0.8$ .

Using this method, we show how the optimal locations of any (reasonable) amount of monitoring units can be approximated in high accuracy and using very little computation resources (less than an hour using a standard server). This method can now be used in order to generate highly accurate approximations of the traffic flow in the network, based on its topology, the OD matrix, and the time to travel without costly simulations. Furthermore, we can also use this method in order to estimate the dynamic changes in optimal deployment due to changes in the betweenness of nodes caused by events such as car accidents and road detours.

In addition, we have solved the monitor placement problem on an artificially produced preferential attachment networks (BA) (Barabasi and Albert 1999) with similar parameters. We have applied the same OD matrix that was computed on the real-world network and arbitrarily chose the first 680 vertices to communicate with each other. We have then used the two algorithms presented in this work on this network. The results of this experiment clearly showed that the optimization problem is more difficult on the real-world transportation network compared to the simulated BA network, despite the fact that both networks had similar parameters and betweenness distribution that followed a power law. Specifically, the GBC of the solutions produced for the random BA model and the provided certificates were lower, and the running time reaches its maximal bound sooner compared to the real-world transportation network. This experiment clearly demonstrates even further the applicability of the proposed method for homeland security usages due to its high accuracy and fast computation time.

In the last section, we have demonstrated that the correlation between the number of monitoring units and the overall monitored traffic percentage can be assessed and extrapolated in a way that enables policy-makers to estimate the minimal number of monitoring units required in order to guarantee a required level of traffic monitoring. This, subsequently, can be used in order to assess also the overall amount of monetary investment required to guarantee a specific level of monitoring, or in other words—to prevent an attack with some assured probability. This linkage between the financial cost of attack prevention and the cost of the attack itself is perhaps the main contribution of this work.

It should be noted that the effectiveness of GBC-based deployment is much higher and the effectiveness of BC-based deployment is much lower in transportation

networks compared to social networks, as reported, for example, in Tubi et al. (2007) (see, e.g., Figs. 3.4 and 3.5 in that paper).

Finally, it is interesting to note that the problem of finding an optimal (and optionally dynamic) deployment for monitoring units is closely related to dynamic decentralized search for evading targets by a flock of unmanned aerial vehicles (UAV). In this problem, however, the fact that the paths of the UAVs are unconstrained (as they are flying in the air) makes the calculation of a near-optimal monitoring strategy fairly easy (see, e.g., an analytically provable suboptimal algorithm in Altshuler et al. (2005b, 2008)). A more theoretical approach to this problem that studies the complexity of all possible strategies for this problem can be found in Altshuler and Bruckstein (2011). An additional similar variant to this problem is the search for pollutant-emitting vehicles, where the merit function is derived from environments considerations (Puzis et al. 2013). It is interesting to mention that in those variants as well, the topological properties of the network along which the “targets” can move significantly influence the ability of monitoring units to track them, as was pointed out in Altshuler et al. (2005a, 2006).

## REFERENCES

- Y. Altshuler and A.M. Bruckstein. Static and expanding grid coverage with ant robots: Complexity results. *Theoretical Computer Science*, 412(35):4661–4674, 2011.
- Y. Altshuler, I.A. Wagner, and A.M. Bruckstein. On swarm optimality in dynamic and symmetric environments. In *Second International Conference on Informatics in Control, Automation and Robotics (ICINCO), the First International Workshop on Multi-Agent Robotic Systems (MARS)*, Barcelona, Spain, pp. 64–71, 2005a.
- Y. Altshuler, V. Yanovski, I.A. Wagner, and A.M. Bruckstein. The cooperative hunters—efficient cooperative search for smart targets using UAV swarms. In *Second International Conference on Informatics in Control, Automation and Robotics (ICINCO), the First International Workshop on Multi-Agent Robotic Systems (MARS)*, Barcelona, Spain, pp. 165–170, 2005b.
- Y. Altshuler, I.A. Wagner, and A.M. Bruckstein. Shape factor’s effect on a dynamic cleaners swarm. In *Third International Conference on Informatics in Control, Automation and Robotics (ICINCO), the Second International Workshop on Multi-Agent Robotic Systems (MARS)*, Setubal, Portugal, pp. 13–21, 2006.
- Y. Altshuler, V. Yanovsky, A.M. Bruckstein, and I.A. Wagner. Efficient cooperative search of smart targets using UAV swarms. *Robotica*, 26:551–557, 2008.
- J.M. Anthonisse. *The rush in a directed graph*. Technical Report BN 9/71. Amsterdam: Stichting Mathematisch Centrum, 1971.
- A-L. Barabasi and R. Albert. Emergence of scaling in random networks. *Science*, 286:509–512, 1999.
- M. Barthélemy. Betweenness centrality in large complex networks. *The European Physical Journal B*, 38(2):163–168, 2004.
- R. Batta and S.S. Chiu. Optimal obnoxious paths on a network: Transportation of hazardous materials. *Operations Research*, 36(1):84–92, 1988.

- S. Bekhor, Y. Cohen, and C. Solomon. Evaluating long-distance travel patterns in Israel by tracking cellular phone positions. *Journal of Advanced Transportation*, 47(4): 435–446, 2013.
- O. Berman, Z. Drezner, and G.O. Wesolowsky. Routing and location on a network with hazardous threats. *Operations Research*, 51(9):1093–1099, 2000.
- D.J. Berndt, A.R. Hevner, and J. Studnicki. Bioterrorism surveillance with real-time data warehousing. In *Proceedings of the first NSF/NIJ Conference on Intelligence and Security Informatics, ISI'03*, Tucson, Arizona, pp. 322–335. Berlin/Heidelberg: Springer-Verlag, 2003.
- G.E.G. Beroggi and W.A. Wallace. Operational control of the transportation of hazardous materials: An assessment of alternative decision models. *Management Science*, 41(12): 1962–1977, 1995.
- P. Bork, L.J. Jensen, C. von Mering, A.K. Ramani, I. Lee, and E.M. Marcotte. Protein interaction networks from yeast to human. *Current Opinion in Structural Biology*, 14(3):292–299, 2004.
- U. Brandes. On variants of shortest-path betweenness centrality and their generic computation. *Social Networks*, 30(2):136–145, 2008.
- H. Chen, F-Y. Wang, and D. Zeng. Intelligence and security informatics for homeland security: Information, communication, and transportation. *IEEE Transactions on Intelligent Transportation Systems*, 5(4):329–341, 2004.
- Committee on Science and Technology for Countering Terrorism and U.S. National Research Council. *Making the nation safer: The role of science and technology in countering terrorism*. Washington, DC: The National Academies Press, 2002.
- L. Damianos, J. Ponte, S. Wohlever, F. Reeder, D. Day, G. Wilson, and L. Hirschman. MiTAP for bio-security: A case study. *AI Magazine*, 23(4):13–29, 2002.
- S. Dolev, Y. Elovici, R. Puzis, and P. Zilberman. Incremental deployment of network monitors based on group betweenness centrality. *Information Processing Letters*, 109:1172–1176, 2009.
- S. Dolev, Y. Elovici, and R. Puzis. Routing betweenness centrality. *Journal of the ACM*, 57(4):25:1–25:27, 2010.
- E. Erkut and A. Ingolfsson. Catastrophe avoidance models for hazardous materials route planning. *Transportation Science*, 34:165–179, 2000.
- E. Erkut and A. Ingolfsson. Transport risk models for hazardous materials: Revisited. *Operations Research Letters*, 33(1):81–89, 2005.
- M.G. Everett and S.P. Borgatti. The centrality of groups and classes. *The Journal of Mathematical Sociology*, 23(3):181–201, 1999.
- M. Faloutsos, P. Faloutsos, and C. Faloutsos. On power-law relationships of the internet topology. *ACM SIGCOMM Computer Communication Review*, 29(4): 251–262, 1999.
- L.C. Freeman. A set of measures of centrality based on betweenness. *Sociometry*, 40(1): 35–41, 1977.
- Y.J. Gur, S. Bekhor, C. Solomon, and L. Kheifits. Intercity person trip tables for nationwide transportation planning in Israel obtained from massive cell phone data. *Transportation Research Record*, 2121:145–151, 2009.
- P. Holme. Congestion and centrality in traffic flow on complex networks. *Advances in Complex Systems*, 6(2):163–176, 2003.

- B.Y. Kara, E. Erkut, and V. Verter. Accurate calculation of hazardous materials transport risks. *Operations Research Letters*, 31(4):285–292, 2003.
- R.E. Korf and W. Zhang. Performance of linear-space search algorithms. *Artificial Intelligence*, 79(2):241–292, 1995.
- J. Lerner. Role Assignments. In *Network analysis: methodological foundations*. Lecture Notes in Computer Science, Vol. 3418. Berlin: Springer-Verlag, 2005.
- F. Lorrain and H.C. White. Structural equivalence of individuals in social networks. *The Journal of Mathematical Sociology*, 1(1):49–80, 1971.
- B. Marshall, S. Kaza, J. Xu, H. Atabakhsh, T. Petersen, C. Violette, and H. Chen. Cross-jurisdictional criminal activity networks to support border and transportation security. In *Proceedings of the seventh IEEE International Conference on Intelligent Transportation Systems*, October 2004, IEEE, pp. 100–105, 2004.
- R. Puzis, Y. Elovici, and S. Dolev. Fast algorithm for successive computation of group betweenness centrality. *Physical Review E*, 76(5):056709, 2007a.
- R. Puzis, Y. Elovici, and S. Dolev. Finding the most prominent group in complex networks. *AI Communications*, 20:287–296, 2007b.
- R. Puzis, M.D. Klipper, Y. Elovici, and S. Dolev. Optimization of nids placement for protection of intercommunicating critical infrastructures. In *EuroISI*, June 2008, Taipei, Taiwan, Springer, 2007c.
- R. Puzis, Y. Altshuler, Y. Elovici, S. Bekhor, Y. Shiftan, and A. Pentland. Augmented betweenness centrality for environmentally-aware traffic monitoring in transportation networks. *Journal of Intelligent Transportation Systems*, 17(1):91–105, 2013.
- P.K. Raj and E.W. Pritchard. Hazardous materials transportation on U.S. railroads: Application of risk analysis methods to decision making in development of regulations. *Transportation Research Record*, 1707:22–26, 2000.
- A.J. Richardson and J. Wolf. Data structures, sampling and survey issues. Report of Workshop M6. In *Ninth International Association of Travel Behaviour Research Conference*, Gold Coast, Australia, 2001.
- J. Scott. *Social network analysis: A handbook*. London: Sage Publications, 2000.
- R. Stern, R. Puzis, and A. Felner. Potential search: A bounded-cost search algorithm. In *AAAI 21st International Conference on Automated Planning and Scheduling (ICAPS)*, Freiburg, Germany, 2011.
- P. Stopher, C.G. Wilmot, C.C. Stecher, and R. Alsnih. Household travel surveys: Proposed standards and guidelines. In *Travel survey methods: Quality and future directions*. Boston: Elsevier, 2006.
- S.H. Strogatz. Exploring complex networks. *Nature*, 410:268–276, 2001.
- The White House. *Homeland security presidential directive/hspd21*. Washington, DC: The White House, 2007.
- M. Tubi, R. Puzis, and Y. Elovici. Deployment of DNIDS in social networks. In *IEEE Intelligence and Security Informatics*, 2007.
- J.G. Wardrop. Some theoretical aspects of road traffic research. In *Proceedings of the Institute of Civil Engineers*, Part II, Vol. 1, ICE Virtual Library of Engineering Divisions, Thomas Telford School, Telford, pp. 325–378, 1952.
- S. Wasserman and K. Faust. *Social network analysis: Methods and applications*. Cambridge, UK: Cambridge University Press, 1994.

- D.R. White and S.P. Borgatti. Betweenness centrality measures for directed graphs. *Social Networks*, 16:335–346, 1994.
- P.D. Wright, M.J. Liberatore, and R.L. Nydick. A survey of operations research models and applications in homeland security. *Interfaces*, 36:514–529, 2006.
- S.H. Yook, H. Jeong, and A-L. Barabasi. Modeling the internet’s large-scale topology. *Proceedings of the National Academy of Science*, 99(21):13382–13386, 2002.
- S. Zilberstein. Using anytime algorithms in intelligent systems. *AI Magazine*, 17(3):73–83, 1996.
- K.G. Zografos and K.N. Androutsopoulos. A heuristic algorithm for solving hazardous materials distribution problems. *European Journal of Operational Research*, 152(2):507–519, 2004.



---

# 4

---

## **ADAPTIVE RESILIENCE AND CRITICAL INFRASTRUCTURE SECURITY: EMERGENT CHALLENGES FOR TRANSPORTATION AND CYBERPHYSICAL INFRASTRUCTURE**

CORRI ZOLI<sup>1</sup> AND LAURA J. STEINBERG<sup>2</sup>

<sup>1</sup>*Institute for National Security and Counterterrorism (INSCT), College of Law/Maxwell School of Citizenship & Public Affairs, Syracuse University, Syracuse, NY, USA*

<sup>2</sup>*College of Engineering and Computer Science, Syracuse University, Syracuse, NY, USA*

### **4.1 INTRODUCTION: ADAPTIVE RESILIENCE**

This chapter explores emergent challenges for the transportation sector through adaptive notions of resilience as they apply to critical infrastructure (CI) security. We frame our analysis through an interdisciplinary policy and engineering systems approach as a means to identify next-generation pressures at the technological, institutional, and policy level that will stress and strain both our physical systems and our analytical frameworks for responding to crises.<sup>1</sup> Beyond well-known natural, accidental, and man-made threats (e.g., CBRN, terrorist attacks, floods, and hurricanes), such challenges include

<sup>1</sup>The National Academies (2012) note, “In 2011 the United States was struck with multiple disasters including 14 weather- and climate-related events that each caused more than \$1 billion in damages. Statistics indicate that total economic damages from all natural disasters in 2011 exceeded \$55 billion in property damage, breaking all records since these data were first reported in 1980.”

(i) the increasing volatility of the natural environment, as weather-related events and energy security needs place cascading demands on overtaxed, interdependent CI systems (Meyer et al. 2012); (ii) the resource gap in updating US CI systems, given global economic recession trends and shortsighted and politicized national planning responses; and (iii) the *post hoc* approach to cyber and command and control (supervisory control and data acquisition (SCADA)) systems security that leave many physical–virtual systems, including transportation infrastructure, vulnerable to attacks or accidents. This last challenge, in fact, is a symptom of the larger problem of new technologies outpacing existing government administrative policy and regulation measures. These challenges are essential to face, as Steven Flynn and Sean Burke note, because twenty-first-century global prosperity will be defined by societies that master resilience in their CI systems in the face of both regular and “chronic and catastrophic risks” (Flynn and Burke 2012).

In the post-9/11 era, federal agencies, state-level CI and emergency management departments, community organizations, and even the public as a whole have made gains in fostering resilience in light of terrorist threats and incidents, as well as in natural disasters and emergencies. In its use by US federal agencies responsible for homeland security, resilience is often defined as “the ability of systems, infrastructures, government, business, and citizenry to resist, absorb, and recover from or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance.”<sup>2</sup> Informed by the US Department of Homeland Security’s (DHS) early implementation of the 9/11 Commission policy recommendations in the Homeland Security Act of 2002, practitioners advocate “whole of community” models that coordinate resources, assets, and systems—from communication channels and new technologies for identifying hazards to networks of safety practitioners across all responder disciplines (see Public Law 107 296; DHS 2011; Kean and Hamilton 2004). Academic research has, further, translated these hard-won practical lessons from the post-9/11 era into an expanding, interdisciplinary subfield of resilience research that underscores the role of preparation, identifying dynamic threats, minimizing risks, training proactive responders, and developing a robust culture of response to varied crises.

In many respects, we are, thus, entering into a moment of mature, adaptive resilience that prioritizes a holistic, interdisciplinary, and local community effect-based approach to complex crises. Important recent thinking about resilience has argued for moving beyond an exclusive focus on physical infrastructures to the goal of integrating complex systems, attending to the physical–virtual interface of these

<sup>2</sup>A common definition of resilience is “the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must” (Allenby and Fink 2005). For resilience in homeland security, see Longstaff (2005), Steinberg et al. (2011), and Longstaff et al. (2010), in which the authors define resilience as “the capacity of a system to absorb disturbance, undergo change, and retain the same essential functions, structure, identity, and feedbacks.” For use of the concept by federal agencies, see Kahan et al. (2009), in which they define resilience as “the ability of systems, infrastructures, government, business, and citizenry to resist, absorb, and recover from or adapt to an adverse occurrence that may cause harm, destruction, or loss [that is] of national significance.” The US Department of Homeland Security’s Homeland Security Advisory Council (2006) prioritizes “critical infrastructure resilience (CIR)” as a supplement to critical infrastructure protection (CIP).

systems, and creating resilient communities. At least five resonant lessons are, thus, evident from innovative resilience research and practice: (i) resisting a “crisis mentality,” acceding to an adversary’s strategic goals, or resorting to panic in favor of continued functioning through the crisis; (ii) distinguishing catastrophic events from localized crises and/or criminal activities and mounting appropriate, measured responses in return; (iii) recognizing the intrinsic risks of open rather than closed societies, the practical limits of absolute security, and the unintended consequences of overzealous policies that trade total security for core democratic values (i.e., civil liberties, due process, and privacy); (iv) leveraging the role of the community as a diverse asset and “force multiplier” in crisis mitigation; and (v) knowing the limits of crisis tools—no matter how technologically sophisticated—and, thus, the need for well-trained, critically thinking human operators to continually assess crisis management tools and processes.<sup>3</sup> Resilience, then, does not mean being immune from violence or mounting the perfect defense against all manner of threats, but the capacity for nations and communities to come together when tragedies occur, to recognize the nature and limits of threats and crises, and to refuse mass panic in the face of overwhelming events.

Nevertheless, a great deal of infrastructural preparation—both at the systems engineering level and as a product of successful public policies—goes into making such adaptive resilience possible (Boone and Hart 2012; Comfort et al. 2010). We, thus, argue that CI security requires balance, the combination of responsive public policy, optimally functioning systems (i.e., using such criteria as robust performance, redundancy, responsiveness, and elasticity of systems), and the intangible dimensions of community (i.e., connectedness, strength of social networks in mitigating crisis, institutional memory, human capital capacity, and leadership) (see Longstaff et al. 2010: 6–7; Roe and Schulman 2012; Steinberg et al. 2011: 9). This chapter, further, argues that the trick is to marry the best interdisciplinary thinking on adaptive resilience with greater emphasis on investing in our CI systems—including innovative engineering and construction efficiencies—at the policy, technological, and physical-structural levels.

An additional reason to join engineering and policy perspectives in understanding new challenges in transportation security is the “perfect storm” of macrostructural pressures on CI systems today and the recent fallout for CI of US national security policy pressures. Converging national and homeland security policy frameworks in the post-9/11 moment has, in many respects, folded traditional homeland priorities—and budgets—into the national security agenda (i.e., counterterrorism, nation-building abroad, national surveillance expenditures over bridge repair).<sup>4</sup> CI initiatives are too often deprived of priority status and resources, while such resources go to

<sup>3</sup>Joel Brenner (2013) notes in “Verizon’s newest data breach investigations report for 2013 tells us—yet again—that cyber security depends on people as much as technology.”

<sup>4</sup>White House (2010) notes, “Our national security strategy is, therefore, focused on renewing American leadership so that we can more effectively advance our interests in the 21st century. We will do so by building upon the sources of our strength at home, while shaping an international order that can meet the challenges of our time. This strategy recognizes the fundamental connection between our national security, our national competitiveness, resilience, and moral example.”

feed a still-growing national security apparatus. Likewise, formerly independent homeland and national security agencies are increasingly integrated (i.e., FBI and NSA) in ways that inject an international security framework into once largely domestic agencies. Indeed, part of this trend is the shift in homeland security policy priorities from critical infrastructure *protection* (CIP) to *resilience* itself, which has unwittingly (Committee on Increasing National Resilience to Hazards and Disasters, Committee on Science, Engineering, and Public Policy 2012; Hollnagel et al. 2006) helped to downgrade improving or securing physical assets (i.e., engineered redundancy) as one element in the “total” resilient ecosystem. Such policy shifts are complicated because they are often well intentioned and designed to address perceived imminent, if often inflated, security threats—though they are also a by-product of divisive legislative politics that depart from established best practices or scientific advances. One consequence is the increasing gap between the US government’s ability to invest in the means and mechanisms to effect large-scale infrastructure policy and projects—including innovation in construction processes—and the ability to mobilize political will for such efforts.

The US transportation sector is beset by these structural and policy-level impacts, from deferred and delayed improvements in deteriorating assets and shrinking national budgets to attenuated policy mechanisms for infrastructure maintenance and innovation (American Society of Civil Engineers 2011). These concerns, evident from poor ratings of national transportation networks to cyberattacks against unsecured SCADA systems, expose significant gaps in CI security policy. Indeed, despite the centrality of the transportation system and its global economic implications and despite significant federal investments in resilience coordination, there is a lack of a robust, updated national policy for redressing core weaknesses in this sector—with implications for resilience, security, and US global competitive advantage (Council on Foreign Relations 2012; Szyliowicz 2012; U.S. Government Accountability Office 2012).

## 4.2 TRANSPORTATION SECTOR SECURITY

To address this nexus of issues, we first examine why the diverse transportation sector remains a high-value target for a range of national security threats, including and beyond terrorist adversaries. We then consider the security dimensions of the transportation sector in relation to other CI systems. In short, targeting the transportation sector—as in the September 11, 2001, attacks—strikes at the core of a modern industrial society’s sense of security, stability, and resilience, its ability to bounce back after a crisis.

### 4.2.1 Transportation Sector as Ongoing Terrorist Target

The transportation sector continues to be an attractive target for terrorists and other adversaries, as successful attacks against these systems invariably gain high operational and symbolic significance. Beyond terrorism, industrial and especially

natural disasters—notably Hurricanes Sandy and Katrina—point to the disparate range of risks to this sector, which necessitates coordinated planning and responses. But in many ways, the strongest indication of the security significance of this complex network is in its high-value status for terrorists, who accurately wager that degrading this of all the CI systems goes to the heart of a modern society’s sense of security and resilience.

It is worth recalling the prevalence of the transportation sector as a target, even before 9/11. Since the first attack on the World Trade Center in 1993 that involved Al-Qaeda members, many terrorist attacks (including foiled efforts) focused on striking at the transportation sector in some meaningful way. The 9/11 attacks notoriously used hijacked commercial aircraft. But before this incident, the foiled bombing of Los Angeles International Airport on New Year’s Eve 1999 also involved air transit. Likewise, the failed attack against the USS *The Sullivans* by Yemeni militants on January 3, 2000, targeted maritime waterways, even though the bomb-laden boat sank before detonation. Indeed, that tactic was successfully revived by Al-Qaeda to strike the USS *Cole* on October 12, 2000, that killed 17 US sailors.

Additional transportation-oriented attacks include such failed efforts as the 2007 plot at John F. Kennedy International Airport by a homegrown Guyanese cell that focused on the jet fuel supply pipelines underneath much of New York City; the Bronx plot by four Muslim converts on May 20, 2009, that failed to shoot down military aircraft near the Air National Guard base in Newburgh, New York; the simultaneous New York and London subway bombing attempts that led to the arrest of Najibullah Zazi, his father, and their imam on September 19, 2009; the failed 2009 Christmas bombing of Northwest Flight 253 by Nigerian Umar Farouk Abdulmutallab; and the attempted car bombing at Times Square on May 1, 2010, by Pakistani-born Faisal Shahzad.

While this list is by no means exhaustive, it provides the broad outlines for how highly visible transportation attacks have occurred at a frequent pace before and after 9/11. It also shows how these transportation strikes have occurred in other major cities: from the 2005 London bombings, the coordinated attack on four commuter trains in Madrid in 2004, and the 2006 plot uncovered in the United Kingdom against US-bound airliners to the suicide bus bombing of Israeli tourists at the Burgas Airport, Bulgaria, on July 18, 2012.

#### **4.2.2 Homeland Security and the Transportation Sector**

What makes the transportation sector pivotal in the CI security context are some of its inherent characteristics. The transportation sector is a “metasystem” in two senses: (i) it encompasses a wide array of semiautonomous assets, structures, and organizations (see Table 4.1), including mass transit systems, such as rail, subways, trams, trolleys, bus, and bike trails; road and highway networks, including bridges, tunnels, walkways, culverts, as well as electrical systems, signage, and maintenance facilities; air systems, including airports and air traffic control; navigable waterways, sea and shipping lanes, harbor, canals, seaports, and ferries; inland shipping and transport sectors, as well as pipelines. Not only is this sector internally variegated with many

**TABLE 4.1 DHS 7 US Transportation System Subsectors**

Subsector Modes	Description
Aviation	Aircraft, air traffic control, 450 commercial airports, 19,000 other airports, heliports, and landing strips; civil and joint use military airports, heliports, short takeoff and landing ports, and seaplane bases
Highway infrastructure and motor carrier	Four million miles of roadway, 600,000 bridges, and 400 tunnels; vehicles include automobiles, motorcycles, trucks carrying hazardous materials, other commercial freights, motor coaches, and school buses
Maritime transportation system	Nine-five thousand miles of coastline, 361 ports, 25,000 miles of waterways, and 3.4 million square miles of EEZ and intermodal landside connections, which allow various modes of transportation to move people and goods to, from, and on the water
Mass transit/ passenger rail	Service by buses; rail transit (commuter rail; heavy rail, i.e., subways and metros; and light rail, i.e., trolleys and streetcars); long-distance rail, that is, Amtrak and Alaska Railroad; and other systems, that is, cable cars, inclined planes, funiculars, and automated guideway systems
Pipeline systems	Vast networks of pipeline traversing hundreds of thousands of miles, carrying nearly all nation's natural gas and 65% of hazardous liquids and chemicals: 2.2 million miles of natural gas pipeline, 168,900 miles of hazardous liquid pipelines, and 109 liquefied natural gas processing and storage facilities
Freight rail	Seven major carriers, hundreds of smaller railroads, 140,000 miles of active railroad, 1.3 million freight cars, 20,000 locomotives, and 12,000 trains operate daily; DoD designates 30,000 miles of track and structure as critical to mobilization and resupply of US forces
Postal/shipping	Moves over 574 million messages, products, and transactions daily. Postal and shipping activity is differentiated from general cargo operations by focus on letter/flat mail and small- and medium-sized packages; service from millions of senders to nearly 152 million destinations

moving parts, (ii) it supports and underpins the functioning of other CI systems, from public health, where hospitals and ambulances rely on roadways and air transport, for instance, to the energy and food supply systems, in which resources are distributed via rail, road, and shipping networks (Grübler 1990). When a robust transportation system is targeted, other CI systems are imperiled with implications across all CI systems.

Second, a robust transportation sector also correlates with a nation's economic wealth—both in the developed and developing worlds. Thus, the transportation sector becomes an irresistible target for adversaries bent on economic warfare.

**TABLE 4.2 DHS Critical Infrastructure Resource Center: Responsible Federal Agency and Critical infrastructure (CI) Sector**

Eighteen CI and Key Resources Sector	Sector-Specific Federal Agency (SSA)
Food and agriculture	Department of Agriculture; Department of Health and Human Services
Defense industrial base	Department of Defense
Energy	Department of Energy
Healthcare and public health	Department of Health and Human Services
National monuments and icons	Department of the Interior
Banking and finance	Department of the Treasury
Water	Environmental Protection Agency
Chemical	Department of Homeland Security
Commercial facilities	<i>Office of Infrastructure Protection</i>
Critical manufacturing	
Dams	
Emergency services	
Nuclear reactors, materials, and waste	
Information technology/communications	<i>Office of Cybersecurity and Communications</i>
Postal and shipping	<i>Transportation Security Administration</i>
Transportation systems	<i>Transportation Security Administration</i> <i>United States Coast Guard (maritime)</i>
Government facilities	<i>Immigration and Customs Enforcement/Federal Protective Services</i>

As noted in DHS, Transportation Security Administration (2007), the transportation network moves “large volumes of goods and individuals through a complex network of approximately 4 million miles of roads and highways, more than 100,000 miles of rail, 600,000 bridges, more than 300 tunnels and numerous sea ports, 2 million miles of pipeline, 500,000 train stations, and 500 public-use airports.” This economic centrality is also evident in international development contexts in which transportation deficits are key obstacles to growth and in achieving the United Nations (UN) Millennium Development Goals (MDGs). In estimating returns on investment (ROI) in infrastructure projects in the developing world (which tend to be higher for low-income countries), for instance, economists calculate average returns between 30 and 40% for telecommunications, more than 40% for electricity generation, and 80% for roads.<sup>5</sup>

Third and relatedly, even with debate over what counts as “CI” sectors (Moteff et al. 2003) in recent discussions over the newly added manufacturing and financial sectors, DHS’s 18 CI sectors framework (see Table 4.2) shows a pivotal role for transportation in both knitting together the diverse US economy and in integrating the domestic economy with the global economy via trade and commerce (DHS 2003, 2009, 2010b).

<sup>5</sup>Kingombe (2011) and Estache (2008) noted that infrastructure investment contributed to over half of Africa’s improved growth performance in the 1990–2005.

In this respect, adversaries seeking to target US vulnerabilities seize upon the modern transportation infrastructure in part because it is plugged into global trade and commerce networks—with implications for continued US growth, prosperity, and global influence.

Last, the robustness of the transportation metasystem is one of the most visible symbols of good governance, both at home and abroad, and, as such, demonstrates a government's capacity to provide security, itself a fundamental premise of governance. Even before 9/11, President Clinton's 1998 Presidential Directive (PDD-63) on *CIP* was designed to secure these vulnerable and interdependent systems, recognizing the nation's infrastructure as "critical" to US national security. Updated after 9/11 in 2003 by President Bush in the *Homeland Security Presidential Directive for Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7)*, the security role of infrastructure was made even more evident, as per the Patriot Act, when "CI" systems (physical and virtual) were deemed "so vital to the United States that [their] incapacity or destruction...would have a debilitating impact on security, national economic security, national public health or safety."<sup>6</sup> When the "critical" transportation sector is targeted, it calls into question whether a state can fulfill the basic governmental function of providing security for its citizens.

It is for these reasons—the metasystem status of transportation; its role in modern social, political, and economic life and in the global economy; and its role in security and governance—that the transportation sector stands as a central pillar in CI security and will remain a viable target.

#### **4.3 EMERGENT THREATS AND COMPLEX CHALLENGES FOR TRANSPORTATION**

We next explore the transportation sector's most proximate challenges with respect to two issues: (i) the limits of the existing national security policy framework for this complex system and its subsectors and (ii) the physical and virtual–physical threats and vulnerabilities that promise to complicate transportation security (Anderson 2009).

At the core of these issues, we believe, is an inability to think creatively and in an interdisciplinary manner about next-generation demands placed on our infrastructure systems. Some demands include (i) the complexity of our interdependent CI systems, both physical and cyber-based systems, vulnerable to new threats, including attacks on SCADA, process control (PCS) and distributed control (DCS) systems; (ii) the immense costs required to secure transportation systems and their components; (iii) the limitations of resilience policy efforts as applied to the transportation security; and (iv) the responsiveness of dispersed

<sup>6</sup>HSPD-7 designates a federal sector-specific agency (SSA) as the lead agency for CI protection efforts in which each SSA develops a sector-specific plan (SSP) that applies the NIPP framework to the unique characteristics of the given sector.

federal agencies and the private sector to identify threats, vulnerabilities, and consequences (Das et al. 2012).

#### **4.3.1 Converging “Security” Policy Frameworks: Implications for Transportation**

To take policy-level challenges first, in the post-9/11 era we have seen not only a convergence in homeland and national security policy agendas, with implications for the traditional domestic CI sector, but a changing national security landscape that has left too little room for investment and innovation in CI protection, particularly at current and projected budget levels. The core of this issue is the dominant notion of national security in externalist, war-based, and overbroad (i.e., global war on terror) terms, which has placed the policy and budgetary focus on overly specific and episodic threats (i.e., Al-Qaeda, terrorism).<sup>7</sup>

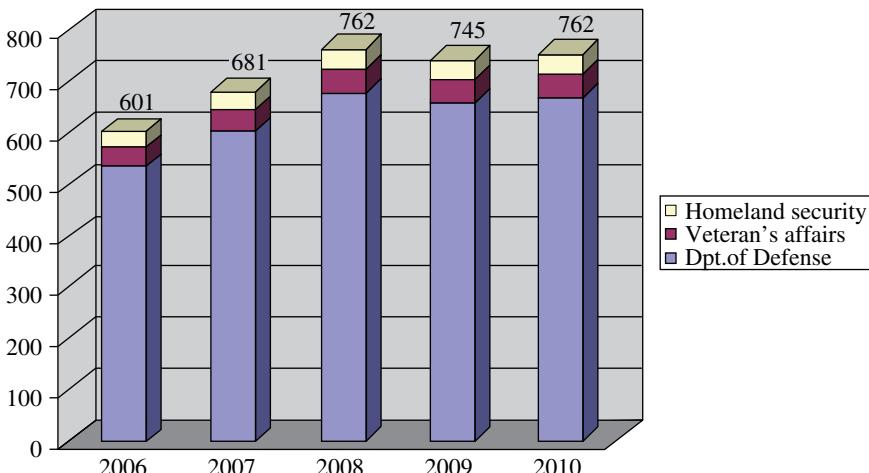
The problems with the national security paradigm for CI are twofold: first, in the past, wartime economies meant heavy investment both in US industrial production capacity, evident in the War Production Board in 1942, and the transportation sector, needed to move rapidly produced items (i.e., munitions, guns, planes, ships, etc.) to operational theaters (Roosevelt 1940). In the post-Cold War period, this is no longer the case. Second, traditionally, national security—or preserving the state from external threats—was posited as the principle goal of states and defined in Cold War terms to mean military power (see Jordan et al. 2011; Waltz 1979, 1993). The term “national security” has since been broadened to include homeland defense, a focus on transnational and irregular threats, and “human security” in which the individual’s welfare (and not only the state) is posited as the salient unit of value for preserving security.<sup>8</sup> In this broader understanding, all aspects of a nation’s interests, values, and instruments of power, as well as an expanded definition of threats (i.e., environmental degradation, transnational crime, infectious disease), are theoretically taken into account in defining a nation’s security policy.

Yet, for historical and institutional reasons, including the slow pace of federal bureaucratic reform and the expanding role of defense industries in setting national priorities, much of the national security policy apparatus is still pitched toward external threats defined militarily.<sup>9</sup> Notably, elemental infrastructure issues at the heart of US economic security and that underpin US influence abroad—and, hence, enhance national and international security—have not been prioritized in this post-9/11 definition of security. Thus, while our theoretical concept of “security” is

<sup>7</sup>For a policy document that captures this converging agenda, see DHS (2010a).

<sup>8</sup>For milestone essays in the expanding concept of national security, see Ullman (1983), Bock and Berkowitz (1966), Knorr (1973), Buzan (1984), Mearsheimer (1992), Walt (1991), Nye and Lynn-Jones (1988), Schultz et al. (1993), Baldwin (1997), and Owen (2004).

<sup>9</sup>As Gordon Lederman (2009) notes, “National security threats in the twenty-first century, such as terrorism, proliferation, failing states, and climate change, are fast, dynamic, and complex. Meeting them successfully requires a capacity to integrate all instruments of U.S. national power—diplomacy, military force, intelligence, law enforcement, foreign aid, homeland security, education, transportation, and health and human services—into a single system supporting a common mission” Lederman goes on to note that despite public servants’ best efforts, our government is “not organized to deliver integrated performance” to meet the range of “existential threats” that we face.



**FIGURE 4.1** DHS as portion of US defense spending 2006–2010. (Source: For a discussion of these numbers, see Office of Management and Budget 2009.)

becoming more inclusive, at the policy level, traditional, external, and national security threats still justify the lion’s share of attention, including at the budgetary level.<sup>10</sup>

Two resonant examples highlight this state of affairs: discrepant investments in “nation-building” at home and abroad in postconflict settings and the “D+” rating by the American Society of Civil Engineers’ (ASCE) *2013 Report Card* on the nation’s transportation infrastructure. From the perspective of CI and transportation investments, over the last decade plus of the wars in Afghanistan and Iraq, postconflict reconstruction and other contingency efforts have been expansive and costly, with estimates at over 1.4 trillion dollars spent, on top of steadily rising Department of Defense (DoD) budgets in the post-9/11 years<sup>11</sup> (see Fig. 4.1 on DHS budget trends, as a share of DoD expenditures). Such investments have also been telling. As

<sup>10</sup>Several recent reports have bemoaned the “opportunity costs” of war and defense overexpenditures. See Crowley (2007).

<sup>11</sup>Operation Enduring Freedom (OEF), beginning in the weeks following September 11, 2001, and still ongoing, and the Iraq intervention or Operation Iraqi Freedom (OIF), March 20, 2003–December 15, 2011, with security assistance still underway. For cost estimates, see Bilmes (2013) and Belasco (2011). According to Belasco, with the sixth FY 2011 Continuing Resolution through March 18, 2011 (H.J.Res. 48/P.L. 112-6), the Congress has approved \$1.283 trillion for military operations, base security, reconstruction, foreign aid, embassy costs, and veterans’ healthcare for the three operations initiated since the 9/11 attacks: OEF Afghanistan and other counterterror operations; Operation Noble Eagle (ONE), providing enhanced security at military bases; and OIF. Of this \$1.283 trillion, CRS estimates that Iraq will receive \$806 billion (63%), OEF \$444 billion (35%) and enhanced base security about \$29 billion (2%), with about \$5 billion that CRS cannot allocate (1/2%). About 94% of the funds are for DOD, 5% for foreign aid programs and diplomatic operations, and 1% for medical care for veterans.

Inspector Generals and Government Accountability Office (GAO) reports confirm, US heavy investments in Iraq and Afghanistan reconstruction, much of which were CI projects, are replete with rampant waste and corruption, while homeland infrastructure project and budgets have languished at home (Rosenberg 2012).

To date, the United States has invested more than 60 and 117 billion, respectively, in reconstruction in Iraq and Afghanistan or, in the case of Iraq, 15 million dollars per day over 9 years of war. For comparison, the United States spent 35 billion in 2010 dollars in rebuilding Germany after World War II from 1946 to 1952 (see Bowen 2013b; Brinkley 2013; Face the Facts USA 2013). Categorizing OIF/OEF expenditures and producing accurate numbers are difficult processes, given unprecedented theft, waste, fraud, and abuse, chronicled by the congressionally mandated Offices of the Special Inspector General for Iraq Reconstruction (SIGIR) and Special Inspector General for Afghanistan Reconstruction (SIGAR).<sup>12</sup> Nevertheless, SIGIR head Stuart Bowen estimates that at least 8 billion or 15% of US total reconstruction costs were lost in Iraq—a figure that does not include SIGIR’s final assessment that most funded programs failed at some level.<sup>13</sup> The Commission on Wartime Contracting in Iraq and Afghanistan puts that number at \$31–60 billion lost to contract waste and fraud in US contingency operations in Iraq and Afghanistan—much of which were large-scale infrastructure projects (Commission on Wartime Contracting in Iraq and Afghanistan 2011). In Iraq, for instance, a large portion of the \$21 billion of the Iraq Relief and Reconstruction Fund (IRR) was spent on traditional infrastructure projects, such as electricity, water supply, roads, housing, etc., though other funds, notably the \$20 billion spent on security forces (ISFF) and \$4 billion of the Commander’s Emergency Response Program (CERP), also comprised large infrastructure programs (see Fig. 4.2 itemizing those fund’s expenditures including infrastructure in SIGIR’s final report) (see Bowen 2013b: 58). While these resources were spent abroad, very little durable investments—or its by-products—were invested in the US industrial economy or its CI.

By contrast, while US expenditures on infrastructure in Iraq and Afghanistan amount to tens of billions of dollars in “easy money” over the last decade plus, most analysts attest to various levels of austerity, decline, and even crisis (National Surface

<sup>12</sup>Coordinated with the Offices of the Inspector General at the DoD, state, and USAID and reporting directly to the Congress, both SIGIR and SIGAR are the US government’s oversight authorities on Iraq and Afghanistan reconstruction created by the Congress to monitor reconstruction funds. SIGIR was created in October 2004 by a congressional amendment to Public Law 108-106 as the successor to the Coalition Provisional Authority Office of Inspector General (CPA-IG); and SIGAR was created by the Congress under the authority of Section 1229 of the National Defense Authorization Act for Fiscal Year 2008 (P.L. 110-181).

<sup>13</sup>Bowen (2013a): “The United States has spent over \$53 billion for thousands of projects to rebuild Iraq, yet, despite 6 months of effort in analyzing agencies’ data, SIGIR was only able to identify a plurality of the projects funded by the five principal appropriations funds...incomplete and Unstandardized databases left us unable to identify the specific use of billions of dollars...Nevertheless, based on the 390 audits and inspections and over 600 investigations conducted by SIGIR’s audit, inspection, and investigative staff since 2004, our judgement (sic) is that waste would range up to at least 15% of Iraq relief and reconstruction spending or at least \$8 billion.”

Relief and reconstruction (IRRF)			Security forces (ISFF)			Commander's emergency (CERP)		
IRRF sector	Obligated	Expended	Project category/fiscal year	Obligated	Expended		Obligated	Expended
Subtotal	2,227.7	2,227.7	Water and sanitation	673.8	227.8	Equipment and transportation	5,327	5,277
Security and law enforcement	4,918.4	4,892.3	Protective measures	490.6	268.1	Infrastructure	3,075	2,972
Electric sector	4,125.5	4,089.1	Electricity	444.7	134.5	Sustainment	2,894	2,620
Justice, public safety infrastructure, and civil society	2,310.0	2,218.3	Education	428.8	180.1	Training and operations	723	698
Water resources and sanitation	1,965.0	1,961.4	Transportation	386.1	150.0	Subtotal	12,018	11,518
Oil infrastructure	1,596.8	1,593.4	Civic cleanup activities	240.9	117.6	Equipment and transportation	2,026	1,945
Private sector development	860.0	830.0	Other urgent humanitarian or reconstruction projects	224.5	84.9	Infrastructure	1,347	1,260
Health care	808.6	805.4	Agriculture	208.5	76.2	Sustainment	663	623
Education, refugees, human rights, democracy, and governance	515.9	447.7	Economic, financial, and management improvements	183.4	77.7	Training and operations	2,656	2,592
Transportation and telecommunications projects	469.8	469.8	Health care	152.5	61.7	Subtotal	6,692	6,420
Roads, bridges, and construction	280.9	280.7	Rule of law and governance	113.4	46.2		859	825
Administrative expenses	219.5	217.9	Civic infrastructure repair	67.5	23.9			
ISPO capacity development	44.9	42.3	Repair of civic and cultural facilities	62.9	27.4			
Subtotal	18,115.3	17,848.4	Civic support vehicles	58.5	33.7			
	20,343.0	20,076.0	Condolence payments	50.8	35.5			
			Telecommunications	39.6	10.2			
			Temporary contract guards for critical infrastructure	35.6	35.3			
			Battle damage repair	23.8	18.0			
			Food production and distribution	21.2	8.2			
			Non-FMR	5.8				
			Detainee payments	1.0	0.6			
			Iraqi hero payments	0.7	0.7			
			Subtotal	3,914.4	1,618.1			

**FIGURE 4.2** SIGIR report on total IRRF, ISFF, and CERP infrastructure expenditures as of September 30, 2012. (Source: DHS 2015 and also see Bowen 2013, SIGAR, Tables 4(2), 4(3) and 4(5).)

Transportation Policy and Revenue Study Commission) in statewide CI investments, especially in transportation. A final report by the National Surface Transportation Policy and Revenue Study Commission, for instance, estimates that the United States must invest at least \$225 billion annually for the next 50 years to repair, upgrade, and advance the surface transportation system—with long-term national economic consequences if the government fails to act.<sup>14</sup> Thus, while the Obama administration has stated that infrastructure is a key investment needed for long-term US economic growth and influence, 2006 and 2007 data show that the US government expenditure on infrastructure dropped to about 2.4% of its GDP, while Europe spends 5% and China spends about 9% of their respective GDPs (Council on Foreign Relations 2013). In fact, one can see in Figure 4.3 that for the president's FY 2013 budget, transportation amounts to only 2%—where military spending garners approximately half of the total federal discretionary budget.<sup>15</sup>

Not only have investments in CI systems at home—bridges and high-speed rail projects are notorious examples—been deferred or delayed, infrastructure investments have often been scaled back to a degree that has left certain sectors surprisingly vulnerable or allowed certain projects, given shrinking budgets, to become derailed due to politicized efforts. It should be obvious that it is exceedingly difficult to make CI systems resilient—let alone a basic institutional feature of US federal response agencies in ways that homeland security communities recommend—when the basic health of our transportation sector is in serious question.<sup>16</sup>

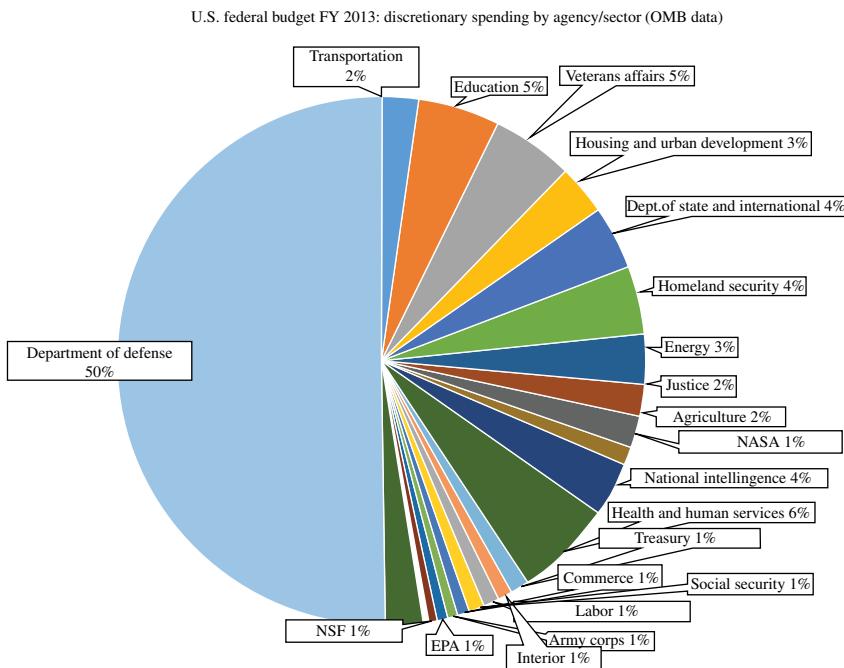
#### **4.3.2 Resilient Transportation Infrastructure: Challenges for the Physical Infrastructure**

The engineering approach to the dual challenges of transportation protection and resilience has generally been characterized by a desire to meet these challenges head-on. As described earlier however, these ambitions can be derailed by a political and policy climate in which infrastructure improvement is chronically underfunded. Engineers and operators have long been aware of the need for infrastructure that is resilient to extreme environmental conditions like hurricanes, high winds, and seismic hazards, but they are facing new challenges not imagined by earlier generations of transportation professionals. Resilience to sea level rise, extended periods of high temperatures in many regions, dramatic changes in rainfall, new patterns of

<sup>14</sup>The Congressional Budget Office (2010), p. ix, noted in FY 2007 (earliest data) that the total public spending for all surface transportation (highways, mass transit, rail, waterways) and water infrastructure was \$356 billion, or 2.4% of the nation's economic output or GDP by combined spending by federal, state, and local governments.

<sup>15</sup>Note that in President Obama's new proposed federal budget (FY 2015), the Department of Transportation sees an increase in funding support. See Office of Management and Budget (2014).

<sup>16</sup>See DHS (2010b), which notes: “The Transportation Security Administration (TSA) and the United States Coast Guard (USCG) are the Sector-Specific Agencies (SSAs) for the Transportation Systems Sector. TSA and the USCG, in collaboration with the Department of Transportation coordinate the preparedness activities among the sector’s partners to prevent, protect against, respond to, and recover from all hazards that could have a debilitating effect on homeland security, public health and safety, or economic well-being.”



**FIGURE 4.3** US government federal discretionary spending budget FY 2013. (Source: For data sources, see the Office of Management and Budget 2012.)

energy use and demand, protections demanded by new modes of transportation and intelligent vehicle systems, and the omnipresent threat of terrorist attacks are defining characteristics of this new reality.

One expression of the engineering reaction to these challenges is the emergence of the “multihazard” design approach in which features of resilient design are used to address several threats simultaneously (e.g., blast proofing, which simultaneously increases resilience to earthquake forces, or aerodynamically designed lead cars, which reduce energy use and CO<sub>2</sub> generation from railways). Another expression is the renewed emphasis on systems analysis, a methodology and perspective that focuses on the interdependencies between components of an infrastructure system and maps the complexities of the local, regional, and national “systems of systems” that depend so strongly on the transportation sector’s resilience (Steinberg et al. 2011). Indeed, it is only by exploiting a systems perspective that a realistic picture of the cascading influence of disruptive forces throughout infrastructure networks can be achieved. This understanding is of paramount importance in modeling and assessing the effectiveness of new design techniques for achieving resilience. Herein lies another area of exploration for the engineering community: how shall resilience be measured and how will we know when our infrastructures have achieved it? The answer will likely be partially dependent on answers from

policy-makers and the public to questions like: what “level” of resilience is desired, what aspects of resilience are most important, and how much are we willing to pay for resilience—not to mention security? As discussed in the previous section, the United States has not been generous in allocating the funding needed to support a transformed transportation infrastructure.

In addition to these considerations, the dizzying array of transportation infrastructure in the United States combined with the opportunity for multimodal choice for consumers of transportation services make the design and analysis of resilient transportation systems extraordinarily difficult. Instead of system-wide resilience, the type of resilience that is often achieved is that of component resilience (i.e., the resilience of an individual bridge or bus station or switching yard)—a practice that leaves the overall system vulnerable to damage or failure through its underdesigned or underprotected sections. It is for this reason that systematic and comprehensive risk assessment is a vital part of transportation infrastructure protection; using measures of risk or relative risk, system components are prioritized for protection based on the likelihood of attack or failure and consequences of such failure. Consequences are often measured in human lives lost, economic disruption, and effects on environmental sustainability (American Association of State Highway and Transportation Officials 2002; Frazier et al. 2009; U.S. Government Accounting Office 2013).

In terms of the sheer amount of infrastructure to protect, there is little doubt that the US highway system, with 600,000 bridges and hundreds of highway tunnels, is the most decentralized of our physical transportation infrastructure (Federal Highway Administration 2003). While sectors such as air transport and ports have been sensitive to security needs for a long time, the highway sector began moving aggressively in this area in the last decade, with nearly coincident attention to the newly emerging threats from climate change (*The Economist* 2011). For the sake of illustration of frameworks for protecting transportation infrastructure, we focus on the highway system, and specifically bridges, in the remaining portion of this subsection (Jaffe 2013).

#### **4.3.3 Securing the Highway Sector**

In a manner similar to that of other portions of the transportation infrastructure, the highway sector uses a two-pronged approach for physical infrastructure resilience: (i) resilience through design or retrofit and (ii) resilience through operational processes. In designing for resilience, highway sector engineers and planners use design criteria that call for the infrastructure to function in expected normal and in extreme environmental conditions. These criteria often incorporate estimates of sea level rise, higher temperatures on the roadways and in bridge and tunnel structures, the properties of new building materials, and changes in population density. These criteria require new calculations of increasing water surfaces and depths, acceptable locations for footings in topographies that may change over time, evolving soil characteristics, higher clearances for bridges, strength estimates for new materials, capacity requirements, and other engineering parameters.

More broadly, with emphasis on reducing costs and building sustainable communities, the designers or planners are often asked to justify whether a particular component is required at all: perhaps transportation needs can be met by a more environmentally sustainable mode, or changes in land use can be employed to reduce the demand function for transportation in the region. Life-cycle costing is a common tool used to assess design options. In a life-cycle analysis, the cost of operating and maintaining infrastructure is added to the construction cost, and the total life-cycle cost is used to select project design. This type of analysis can advantage more resilient designs, as the resilience features may be utilized later in the design life of the project (e.g., those that account for future climate change or that utilize more sustainable materials).

“Resilience through design” is also used to address the need to secure a structure, and the people in it or on it, from attack. Bridges represent key nodes in transportation systems and are particularly attractive targets for terrorists. As *The New York Times* reported using data from the Guantanamo files, “Al Qaeda has long had a fascination with suspension bridges … Khalid Shaikh Mohammed the admitted mastermind of the [9/11] attacks got even more explicit, telling an operative to ‘destroy the Brooklyn Bridge by cutting the suspension cables’” (Weiser and Baker 2011). Other documents from Guantanamo speak of “methods to destroy suspension bridges” and the targeting of “major hanging bridges” (Weiser and Baker 2011).

Physical threats to bridges include explosive devices, cutting devices, impact vehicles, critical utilities running on bridges, and specific vulnerable attack locations. There are a variety of structural measures used to protect against attacks from these threats, including the use of strong and ductile materials (e.g., concrete of high compressive strength and particularly ductile grades of steel, additional reinforcement on concrete deck slabs and columns, bracing and steel cabling, enhanced footing design, use of new blast-resistant materials such as elastomeric coatings, and shielding of cables) (Sharp and Clemena 2004; Williamson and Winget 2005). Design criteria for effectively resisting attacks have been developed from experimental blast results, modeling and simulation of blast impacts, and analyses of prior attacks. Programs for developing new materials and efforts at creating “self-healing” and “self-monitoring” structures are actively underway as part of the national effort to secure CI (Domich 2010).

Beyond design and retrofit for security, the transportation sector guards infrastructure with a wide range of physical security countermeasures.<sup>17</sup> These include key control and locks, strategically placed fencing and antiram barriers, protective lighting, alarm systems, electronic access control systems, and surveillance monitoring. Security forces are often permanently deployed at major bridges (Weiser and Baker 2011), and there are often employee watch programs and security trainings for employees, including training in the capability to identify suspicious activity and recognize behaviors associated with reconnaissance. Emergency response plans will be in place and practiced.

<sup>17</sup> See Mark Prado (2011) for an example of physical security measures at the Golden Gate Bridge and Frazier et al. (2009).

#### 4.3.4 Transportation Challenges at the Cyberphysical Interface: Vulnerable SCADA Control Systems

There is an emergent bright spot in CI and homeland security budgets in which significant investments—and accompanying pushes for innovation—are on the national agenda: cybersecurity. As various agencies have reported, the recent 2013 DHS budget of \$60 billion (see DHS 2012) shows a 74% rise in cyber expenditures, while the overall department funding has remained constant.<sup>18</sup> Additional funds have been earmarked for state-based cybersecurity initiatives, education and training programs for a cybersecurity workforce, research, cyber investigations, and incident reporting (Sadasivan 2013).

While there is no question that securing the cyberphysical interface of CI is a national priority, the problem over the last several years has turned on the integrity of industrial control systems (ICS)—the wide variety of computer-based networked systems that monitor and control industrial processes that exist in the physical world, especially SCADA systems.<sup>19</sup> SCADA systems are different from other control systems in that they are the metacontrol systems for widely dispersed sites or facilities, whether manufacturing and production sites, water distribution, oil and gas pipelines, electrical power transmission, or civil defense siren systems (Zhu et al. 2011). In running large-scale industrial processes that involve multiple sites and vast distances, SCADA systems “supervise” the linked, local, automatic remote terminal units (RTUs) and programmable logic controllers (PLCs) that use sensors to exchange data about site-specific processes. So a PLC may control the local flow of cooling water in a nuclear facility, but it sends its data to be monitored to the central SCADA system, along with all other nuclear facilities and their local systems, where human operators then review and change set points or create alerts and generally assess the overall performance of all systems in the loop.

The problem with control and SCADA systems are cyber threats—a problem that is at its core technical (see Fernandez et al. 2009). That is, SCADA systems were designed to be open, to invite human interaction, and thus to work at the human-machine interface; hence, security was a structural afterthought. Moreover, the SCADA architecture has itself adapted along with other technological advances, thus inheriting security vulnerabilities at each phase (Alcaraz and Zeadally 2013). First-generation mainframe-based independent systems, for instance, were not connected to other systems (and had backup systems); second-generation distributed systems were connected to a limited number of local area network (LAN) computers; while

<sup>18</sup>These initiatives include, for instance, \$236 million for improved federal agency network security in accordance with the Federal Information Security Management Act; \$345 million for the National Cybersecurity Protection System (NCPS), known as EINSTEIN, an intrusion prevention system within the Comprehensive National Cybersecurity Initiative mission; and \$93 million for US-CERT Operations, the operational arm of the National Cyber Security Division.

<sup>19</sup>Depending on the application, control systems include process control systems (PCS), supervisory control and data acquisition (SCADA) systems in industries and critical infrastructures, and cyberphysical systems (CPS) or the embedded sensors and actuator networks between systems. Most industrial control systems have a hierarchical structure and are composed of a set of networked agents, consisting of sensors, actuators, control processing units, and communication devices (Cárdenas et al. 2008).

present third-generation Internet networked systems are accessed through the Internet and thus vulnerable to remote attack. An additional problem is changing communication or telemetry protocols. Where SCADA systems had used low-bandwidth radio and direct wired connections, the proprietary communication protocols used in second-generation systems have shifted to now standardized third-generation systems, which have been adapted to operate over the Internet's standard communication protocol (i.e., Transmission Control Protocol and the Internet Protocol (TCP/IP)).<sup>20</sup> Use of the Internet's system of digital rules for message exchange between networks and its physical infrastructure (i.e., wireless and fiber-optic cables) enables a direct link between the Internet and industrial networked communications in ways that prevent SCADA systems from being self-contained.<sup>21</sup> As Bonnie Zhu et al. note, “Remote locations and proprietary industrial networks used to give SCADA system a considerable degree of protection through isolation” (Zhu et al. 2011).<sup>22</sup> This is no longer true.

To complicate matters, cyberattacks in general are notoriously stealthy—making attribution nearly impossible—and in SCADA systems, they involve unauthorized access via control software, networks, and physical systems. Analysts are beginning to study how these attacks have occurred (i.e., at the Maroochy Shire Council’s sewage control system in Australia, as well as the Stuxnet and Aramco attacks), and many SCADA vendors have tried to remedy these risks with specialized solutions for TCP/IP-based SCADA networks, external SCADA monitoring equipment, advanced encryption, and even hardware-installed “bump in the wire” authentication devices, as organizations like the International Society of Automation (ISA) have increasingly formalized security recommendations and requirements.

In addition to these technically derived issues of systems security and attribution, however, the broader policy challenges that we have laid out here are significant, insofar as they create added obstacles (wittingly or not) for solving technical deficits. These include a patchwork quilt of federal cyber authorities and policies that do not adequately regulate cyberspace and the fact that the vast majority of the nation’s information infrastructure is owned and operated by the private sector, which makes establishing regulations (with their attending protections for privacy, proprietary) difficult. The federal government has long recognized this problem and, through the Office of Infrastructure Protection in the DHS, has established an interlocking web of sector coordinating councils with representatives from key industry leaders and coordinating personnel from the DHS and other relevant agencies, sector-specific government coordinating councils populated by government leaders drawn from

<sup>20</sup>These baseline digital rules for message exchange within and between computers (i.e., the Internet Protocol suite) is the original networking model that defined communication protocols used for the Internet and similar computer networks; it is also referred to by computer scientists as the DoD standard because of the role of the Advanced Research Projects Agency Network (ARPANET) (later DARPA) in developing and implementing this standard.

<sup>21</sup>Efforts such as the North American Electric Reliability Corporation (NERC) and DHS critical infrastructure protection recommendations (i.e., using satellite-based communication) have attempted to mitigate these vulnerabilities.

<sup>22</sup>The US Computer Emergency Readiness Team (US-CERT) has issued vulnerability advisories on SCADA software, as well as patches.

across the federal government, cross-sector councils, regional coordinating councils, and other councils. This large and somewhat unwieldy structure of networks of infrastructure protection stakeholders serves primarily to encourage information sharing and to provide fora for planning mitigation measures and responses to infrastructure threats. However, as many commentators point out, these public–private partnerships (PPPs) are not necessarily effective in motivating the private sector to take action for infrastructure protection (see, e.g., Auerswald et al. 2005; Givens and Busch 2013).

The uneven record of PPPs in motivating infrastructure protection measures in the private sector is due in part to a divergence of goals: the government is primarily concerned with “CIP” as a public good, while private industry looks first to ensure its own “continuity of operations.” As described by Boyer et al. writing for the US Chamber of Commerce, “identifying risks in PPP planning does not guarantee that the private sector will adopt plans to deal with them. … Since PPPs depend on a business model, the high costs of certain risks will determine whether they will be transferred from public to private sectors. Disasters, once identified and considered, may prove too high a cost for the private sector to bear” (Boyer et al. 2012). Showing an appreciation for the exigency needed to address the cybersecurity threat, President Obama signed Executive Order 13636 in February 2013, which acknowledges the need to establish market-based incentives to encourage the participation of private industry in cybersecurity. Among the incentives that are proposed are cybersecurity insurance, liability limitations, public recognition, and cooperative research on cybersecurity protection.

In fact, in many respects, CI cybersecurity challenges have tested the mettle of the twin policy concepts of public–private partnerships and “whole of government” approaches to security and resilience in ways that have not shown government performance in a favorable light. Beyond the privately owned and operated information infrastructure, there is also a severe shortage of cybersecurity talent for CI defense in ways that analysts have predicted (Chin and Older 2009; Devendorf et al. 2012; Jabbour 2010). In these ways, CI cybersecurity challenges have the potential to reiterate the “perfect storm” problems outlined earlier in which policy shifts and technical challenges conspire to make today’s infrastructure problems exceedingly difficult to solve.

#### 4.4 CONCLUSION: TRANSPORTATION SECURITY AT A CROSSROADS

There should be little doubt that given present challenges for the transportation sector, an interdisciplinary—policy–technical—approach to infrastructure security is necessary. This approach should take into account CI protection and resilience, national policy planning as well as systems capacity building, and recommendations for new and more effective methods in securing CI based on “systems of systems” perspectives on challenges and solutions. We have also emphasized the critical role of research—including identifying national priority issues—to focus such multisectoral efforts and in pushing toward a unity of effort in building security into existing CI systems and processes.

At the heart of this discussion, however, is the need to apply critical concepts of adaptive resilience to public investments in our CI systems, beginning with surface transportation. As many analysts have pointed out, the crisis in US infrastructure ultimately informs these systems' security and, thus, is a problem of national scale: they include lost productivity, sluggish economic recovery, lost opportunity costs, global competitiveness, as well as the combined costs of failing to act (Laing 2012; Plumer 2013; Sledge 2012). In fact, the ASCE's recent report, *Failure to Act: The Impact of Current Infrastructure Investment on America's Economic Future*, quantifies the cost of our decaying infrastructure systems, including transportation (American Society of Civil Engineers 2011: 8). In addition to the costs of subpar or deteriorating surface transportation systems, which cost \$130 billion in 2010, the report projects that the overall costs of failing to invest in the nation's roads and bridges by 2020 will total \$3.1 trillion in lost GDP growth and 877,000 lost jobs. Those costs, that is, arise less from a dramatic failure in a given system, such as the recent I-35W bridge collapse in Minnesota, but from "mundane" problems: congestion and traffic jams that increase shipping and fuel costs, closed bridges and rerouted traffic, declining business sales across industries from entertainment to health services, and the wear and tear on transportation vehicles from deficient roadways (Sledge 2012).

Thus, applying an interdisciplinary and adaptive resilience approach enables us to see that we need to contemplate such challenges with some of these hard-won insights: first, we need to resist a "crisis mentality," the perspective of panic or powerlessness, in favor of high-functioning processes that develop a multisectoral plan for CI security progress. While, no doubt, changing the fuel tax–highway funding policy and private–public matching funds will be part of such progress, CI investments cannot depend upon the pace of legislative activity or even bureaucratic reform. Second, we need to distinguish catastrophic events, many of which include an element of surprise or strategic motivation, from truly man-made crises that require urgent, systematic, and measured responses. In the case of transportation, there is no possibility for CI security without needed investments in getting the mass transit systems up to par, especially in critical need areas (highways, bridges) and in emergent threat areas (cyber control systems for surface transportation). Moreover, a good deal of this discussion needs to attend to climate change and energy security issues—problems that have been sorely neglected in public discourse and policy planning. Third, we need to recognize the risks and unintended consequences of inaction and place such risks on an equal level with often prioritized national security risks from foreign adversaries. Fourth, we need to leverage the role of multiple and diverse communities as a "force multiplier" in transportation security and in mitigating crises in multiple infrastructure systems. These communities include, more obviously, researchers; law- and policy-makers at the local (municipal), state, and federal levels; systems engineers and professional societies; as well as other technical specialists but also unions and prolabor organizations, including the construction sector, business interests and chambers of commerce, international development organizations, and federal agencies beyond the Department of Transportation (i.e., the National Science Foundation, Department of Commerce).

Last, we need to soberly reflect on the limits of our crisis mitigation tools—no matter how technologically sophisticated—which include, unfortunately, elements of the federal policy processes (Bump 2013; Laing 2011). Well-trained, critically thinking human operators will need to fairly assess our crisis management means, mechanisms, and processes and come up with alternatives if and when these show signs of failure. Ultimately, marrying the lessons of adaptive resilience with a push for greater urgency in investing in our CI systems is the recipe for success in meeting CI challenges.

## REFERENCES

- C. Alcaraz and S. Zeadally, “Critical Control System Protection in the 21st Century: Threats and Solutions,” *Computer*, February 14, 2013, IEEE Computer Society Digital Library/IEEE Computer Society.
- B. Allenby and J. Fink, “Toward Inherently Secure and Resilient Societies,” *Science*, 309 (2005): 1034.
- American Association of State Highway and Transportation Officials, *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*. Vienna, VA: Transportation Policy and Analysis Center, Science Applications International Corporation, 2002.
- American Society of Civil Engineers, *Failure to Act: The Economic Impact of Current Investment Trends in Surface Transportation Infrastructure*, August 28, 2011. Available at: <http://www.asce.org/failuretoact/> (accessed February 21, 2015).
- R.S. Anderson, “Cyber Security and Resilient Systems,” *Institute of Nuclear Materials Management 50th Annual Meeting*, INL/CON-09-16096, Idaho Falls, ID: Idaho National Laboratory, July 2009. Available at: <http://www.inl.gov/technicalpublications/Documents/4311316.pdf> (accessed February 27, 2015).
- P. Auerswald, L.M. Branscomb, T.M. La Porte, and E. Michel-Kerjan, “The Challenge of Protecting Critical Infrastructure,” *Issues in Science and Technology*, 22 (Issue 1) (Fall 2005): 77–83.
- D. Baldwin, “The Concept of Security,” *Review of International Studies*, 23 (1997): 5–26.
- A. Belasco, *The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11*, CRS Report RL33110. Washington, DC: Congressional Research Service, 2011.
- L. Bilmes, “The Financial Legacy of Iraq and Afghanistan: How Wartime Spending Decisions Will Constrain Future National Security Budgets,” *HKS Faculty Research Working Paper Series*, RWP13-006. Cambridge, MA: Harvard Kennedy School, March 2013.
- P.G. Bock and M. Berkowitz, “The Emerging Field of National Security,” *World Politics*, 19 (1966): 124.
- E.W. Boone and S.D. Hart, *Full Spectrum Resilience*. Alexandria, VA: The Infrastructure Security Partnership, 2012. Available at: <http://www.tisp.org/index.cfm?cdid=12624&pid=10261> (accessed February 21, 2015).
- S.W. Bowen, Jr., *Government Agencies Cannot Fully Identify Projects Financed with Iraq Relief and Reconstruction Funds (SIGIR 13-006)*, March 6, 2013a, p. 21. Available at: <http://www.sigir.mil/embargo/files/audits/13-006.pdf> (accessed February 21, 2015).
- S.W. Bowen, Jr., *Learning from Iraq: A Final Report from the Special Inspector General for Iraq Reconstruction*. Arlington, VA: Office of the Special Inspector General for Iraq

- Reconstruction, 2013b, p. 55. Available at: <http://www.sigir.mil/learningfromiraq/index.html> (accessed February 27, 2015).
- E. Boyer, R. Cooper, and J. Kavinoky, *Public-Private Partnerships and Infrastructure Resilience*. Washington, DC: National Chamber Foundation, U.S. Chamber of Commerce, 2012.
- J. Brenner, "Is Anyone Really Responsible for Your Company's Data Security?" *Harvard Business Review Blog Network*, June 19, 2013. Available at: <http://blogs.hbr.org> (accessed February 21, 2015).
- J. Brinkley, "Money Pit: The Monstrous Failure of US Aid to Afghanistan," *World Affairs*, January–February (2013). Available at: <http://www.worldaffairsjournal.org/article/money-pit-monstrous-failure-us-aid-afghanistan> (accessed February 21, 2015).
- P. Bump, "Obama Calls for Infrastructure Spending for the Fifth Time in Five Years," *The Atlantic Wire*, March 29, 2013.
- B. Buzan, "Peace, Power and Security: Contending Concepts in the Study of International Relations," *Journal of Peace Research*, 21 (1984): 109–125.
- A.A. Cárdenas, S. Amin, and S. Sastry, "Research Challenges for the Security of Control Systems," *HotSec 2008, Proceedings of the third Conference on Hot Topics in Security*, No. 6. USENIX Association, Berkeley, CA, 2008. Available at: <http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/cardenas.pdf> (accessed February 21, 2015).
- S-K. Chin and S. Older, "Educating Engineers to Design Trustworthy Systems," *Indo-US Conference and Workshop on Cyber Security, Cyber Crime, and Cyber Forensics*, Kochi, India, August 19–21, 2009.
- L. Comfort, A. Boin, and C. Demchak, *Designing Resilience: Preparing for Extreme Events*. Pittsburgh, PA: University of Pittsburgh Press, 2010.
- Commission on Wartime Contracting in Iraq and Afghanistan, *Final Report to Congress: Transforming Wartime Contracting Controlling Costs, Reducing Risks*. Arlington, VA: Commission on Wartime Contracting in Iraq and Afghanistan, 2011. Available at: [wartimecontracting.gov](http://wartimecontracting.gov) (accessed February 21, 2015).
- Committee on Increasing National Resilience to Hazards and Disasters, Committee on Science, Engineering, and Public Policy, *Disaster Resilience: A National Imperative*. Washington, DC: The National Academies Press, 2012, p. 3.
- Congressional Budget Office, *Public Spending on Transportation and Water Infrastructure*, November 2010. Available at: <http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/119xx/doc11940/11-17-infrastructure.pdf> (accessed February 21, 2015).
- Council on Foreign Relations, *Road to Nowhere: Federal Transportation Infrastructure Policy*, June 2012. Available at: [www.cfr.org/roadtonowhere](http://www.cfr.org/roadtonowhere) (accessed February 21, 2015).
- Council on Foreign Relations, *Research Links: Infrastructure*, February 2013. Available at: <http://www.cfr.org/united-states/infrastructure/p26178> (accessed February 21, 2015).
- P.J. Crowley, *Lost Opportunities: Bush Defense Spending Is Misplaced*. Washington, DC: Center for American Progress, 2007. Available at: [http://www.americanprogress.org/wp-content/uploads/issues/2007/02/pdf/defense\\_report.pdf](http://www.americanprogress.org/wp-content/uploads/issues/2007/02/pdf/defense_report.pdf) (accessed February 21, 2015).
- S.K. Das, K. Kant, and N. Zhang, *Handbook on Securing Cyber-Physical Critical Infrastructure*. Burlington, MA: Elsevier, 2012.
- E. Devendorf, S. Muccio, and F. Wieners, "Developing the Next Generation of Cyber Leaders," *Proceedings of the 16th Colloquium for Information Systems Security Education*, Lake Buena Vista, FL, June 11–13, 2012, pp. 34–41.

- DHS, Critical Infrastructure Resource Center, 2015. Available at: <http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/sectorOverview.htm> (accessed May 9, 2015).
- P.D. Domich, "System and Sector Interdependencies: An Overview of Research and Development," in J.G. Voeller (ed.), *Wiley Handbook of Science and Technology for Homeland Security*. Hoboken, NJ: John Wiley & Sons, Inc., 2010.
- A. Estache, "Infrastructure and Development: A Survey of Recent and Upcoming Issues," in F. Bourguignon and B. Pleskovic (eds.), *Rethinking Infrastructure for Development*. Washington, DC: World Bank, 2008.
- Face the Facts USA, *U.S. Spends More Rebuilding Iraq, Afghanistan than Post-WWII Germany*, George Washington University, Face the Facts Project, January 2013. Available at: <http://www.facethefactsusa.org/facts/us-spends-more-rebuilding-iraq-afghanistan-than-post-wwii-germany/#sthash.uMb20l6I.dpuf> (accessed February 21, 2015).
- Federal Highway Administration, *Recommendations for Bridge and Tunnel Safety*, prepared by the Blue Ribbon Panel on Bridge and Tunnel Security for ASSHTO Transportation Security Task Force, January 2003. Available at: <http://www.fhwa.dot.gov/bridge/security/brp.pdf> (accessed February 21, 2015).
- E.B. Fernandez, J. Wu, M.M. Larondo-Petrie, and Y. Shao, "On Building Secure SCADA Systems Using Security Patterns," *Proceedings of the fifth Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*, Article No. 17. New York: ACM, 2009.
- S. Flynn and S. Burke, *Critical Transportation Infrastructure and Societal Resilience*. Washington, DC: Center for National Policy, 2012. Available at: <http://cnponline.org/ht/a/GetDocumentAction/i/38487> (accessed February 27, 2015).
- E.R. Frazier Sr., Y.J. Nakanishi, and M.A. Lorimer, *Security 101: A Physical Security Primer for Transportation Agencies*, National Cooperative Highway Research Program, Report 525. Washington, DC: Transportation Research Board, 2009.
- A.D. Givens and N.E. Busch, "Realizing the Promise of Public-Private Partnerships in US Critical Infrastructure Protection," *International Journal of Critical Infrastructure Protection*, 6 (2013): 39–50.
- A. Grübler, *The Rise and Fall of Infrastructures: Dynamics of Evolution and Technological Change in Transport*. Heidelberg/New York: Physica-Verlag, 1990.
- E. Hollnagel, D.D. Woods, and N. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*. Aldershot: Ashgate Publishing Limited, 2006.
- K. Jabbour, "CyberVision and Cyber Force Development," *Strategic Studies Quarterly*, Spring (2010): 63–73.
- E. Jaffe, "Why America's Bridges Are in Such Dangerously Bad Shape," *The Atlantic: Cities*, June 18, 2013.
- A.A. Jordan, W.J. Taylor, Jr., M.J. Meese, and S.C. Nielsen, *American National Security*, 6th ed. Baltimore, MD: Johns Hopkins University Press, 2011, pp. 3–6.
- J. Kahan, A. Allen, and J. George, "An Operational Framework for Resilience," *Journal of Homeland Security and Emergency Management*, 6 (2009): 1–48.
- T.H. Kean and L. Hamilton, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004.
- K.M. Kingombe, *Mapping the New Infrastructure Financing Landscape*. London: Overseas Development Institute, 2011. Available at <http://www.odi.org.uk/sites/odi.org.uk/files/odi-assets/publications-opinion-files/6311.pdf> (accessed February 21, 2015).

- K. Knorr, "National Security Studies: Scope and Structure of the Field," in F.N. Trager and P.S. Kronenberg (eds.), *National Security and American Society: Theory, Process and Policy*. Lawrence, KS: University of Kansas Press, 1973, p. 5.
- K. Laing, "House Republicans: White House Plan for Infrastructure Bank 'Dead on Arrival,'" *The Hill*, October 10, 2011.
- K. Laing, "CBO Reports Highway Trust Fund Headed for Bankruptcy in 2014," *The Hill*, January 31, 2012.
- G. Lederman, "National Security Reform for the Twenty-first Century: A New National Security Act and Reflections on Legislation's Role in Organizational Change," *Journal of National Security Law & Policy*, 3 (2009): 363–376.
- P.H. Longstaff, *Security, Resilience, and Communication in Unpredictable Environments Such As Terrorism, Natural Disasters, and Complex Technology*. Cambridge, MA: Program for Information Resources Policy, Harvard University, 2005.
- P.H. Longstaff, N. Armstrong, K. Perrin, W.M. Parker, and M.A. Hidek, "Building Resilient Communities: A Preliminary Framework for Assessment," *Homeland Security Affairs*, 6(3) (2010): 3.
- J.J. Mearsheimer, "Disorder Restored," in G. Allison and G.F. Treverton (eds.), *Rethinking America's Security*. New York: W.W. Norton, 1992, pp. 213–237.
- M.D. Meyer, E. Rowan, M.J. Savonis, and A. Choate, *Integrating Extreme Weather Risk into Transportation Asset Management*. Washington, DC: American Association of State Highway and Transportation Officials, 2012.
- J. Moteff, C. Copeland, and J. Fischer, *Critical Infrastructures: What Makes an Infrastructure Critical?* Report for Congress (RL31556). Washington, DC: Congressional Research Service, 2003. Available at: <http://www.fas.org/irp/crs/RL31556.pdf> (accessed February 21, 2015).
- National Surface Transportation Policy and Revue Study Commission, *Transportation for Tomorrow: Report of the National Surface Transportation Policy and Revenue Study Commission*, p. 1. Available at: [http://transportationfortomorrow.com/final\\_report/pdf/volume\\_1.pdf](http://transportationfortomorrow.com/final_report/pdf/volume_1.pdf) (accessed February 21, 2015).
- J.S. Nye and S.M. Lynn-Jones, "International Security Studies: A Report of a Conference on the State of the Field," *International Security*, 12 (1988): 5–27.
- Office of Management and Budget, *A New Era of Responsibility: Renewing America's Promise, Budget of the United States Government, FY 2010*. February 26, 2009. Available at: <http://www.gpo.gov/fdsys/pkg/BUDGET-2010-BUD/pdf/BUDGET-2010-BUD-7.pdf> (accessed May 9, 2015).
- Office of Management and Budget, The Budget of the United States Government, Barak H. Obama. February 13, 2012, with specific "Summary Tables." Available at <http://www.gpo.gov/fdsys/pkg/BUDGET-2013-BUD/pdf/BUDGET-2013-BUD-29.pdf> (accessed May 9, 2015).
- Office of Management and Budget, *Budget of the U.S. Government, FY 2015*. Washington, DC: U.S. Government Printing Office, 2014. Available at: <http://www.whitehouse.gov/sites/default/files/omb/budget/fy2015/assets/budget.pdf> (accessed February 27, 2015).
- T. Owen, "Human Security—Conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold-Based Definition," *Security Dialogue*, 35 (2004): 373–387.
- B. Plumer, "U.S. Infrastructure Spending Has Plummeted Since 2008," *The Washington Post*, May 24, 2013.

- M. Prado, "Golden Gate Bridge 'Hardened' Against Terror Attacks Since 9/11," *Marin Independent Journal*, September 5, 2011.
- E. Roe and P.R. Schulman, "Toward a Comparative Framework for Measuring Resilience in Critical Infrastructure Systems," *Journal of Comparative Policy Analysis: Research and Practice*, 14(2) (2012): 114.
- F.D. Roosevelt, "Arsenal of Democracy," Radio Address Delivered by President Roosevelt, December 29, 1940, Washington, DC. Available at: <https://www.mtholyoke.edu/acad/intrel/WorldWar2/arsenal.htm> (accessed February 27, 2015).
- M. Rosenberg, "U.S. Fund to Rebuild Afghanistan Is Criticized," *The New York Times*, July 30, 2012.
- K. Sadasivan, "DHS' Focus in FY 2014: Cybersecurity and Critical Infrastructure," *Fedscoop*, April 18, 2013. Available at: <http://fedscoop.com/dhs-focus-in-fy-2014-cybersecurity-and-critical-infrastructure/#sthash.ju5FtvSz.dpuf> (accessed February 21, 2015).
- R. Schultz, R. Godson, and T. Greenwood (eds.), *Security Studies for the 1990s*. New York: Brassey's, 1993.
- S.R. Sharp and G.G. Clemena, *State of the Art Survey of Advance Materials and their Potential Application in Highway Infrastructure*, Virginia Transportation Research Council, VTRC 05-R9, November 2004. Available at: [http://www.virginiadot.org/vtrc/main/online\\_reports/pdf/05-r9.pdf](http://www.virginiadot.org/vtrc/main/online_reports/pdf/05-r9.pdf) (accessed February 21, 2015).
- M. Sledge, "Infrastructure Problems in U.S. Go Far Beyond Dollars," *Huffington Post*, February 2, 2012.
- L.J. Steinberg, N. Santella, and C. Zoli, "Baton Rouge Post-Katrina: The Role of Critical Infrastructure Modeling in Promoting Resilience," *Homeland Security Affairs*, 7(7) (2011): 1.
- J.S. Szyliowicz, "Safeguarding Critical Transportation Infrastructure: The US Case," *Transport Policy*, 28 (2012): 69.
- The Economist*, "America's Transport Infrastructure: Life in the Slow Lane," April 28, 2011.
- The National Academies, *Disaster Resilience*. Washington, DC: The National Academies, 2012. Available at: [http://www.nap.edu/openbook.php?record\\_id=13457&page=11](http://www.nap.edu/openbook.php?record_id=13457&page=11) (accessed February 21, 2015).
- U.S. Department of Homeland Security (DHS), *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003. Available at: <http://www.dhs.gov/homeland-security-presidential-directive-7> (accessed February 21, 2015).
- U.S. DHS, *National Infrastructure Protection Plan (NIPP)* (2009). Available at: [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf) (accessed February 21, 2015).
- U.S. DHS, *Quadrennial Homeland Security Review (QHSR) Report 2010: A Strategic Framework for a Secure Homeland*. Washington, DC: U.S. DHS, 2010a. Available at: [http://www.dhs.gov/xlibrary/assets/qhsr\\_report.pdf](http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf) (accessed February 21, 2015).
- U.S. DHS, *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*. Washington, DC: U.S. DHS, 2010b. Available at: <http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf>; [http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/assets/SSP\\_TransportationSystems.pdf](http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/assets/SSP_TransportationSystems.pdf) (accessed February 27, 2015).
- U.S. DHS, *Implementing 9/11 Commission Recommendations: Progress Report* (2011). Available at: <http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf> (accessed February 21, 2015).

- U.S. DHS, *Written Testimony of DHS Secretary Janet Napolitano for a Senate Committee on Homeland Security and Governmental Affairs Hearing on the President's Fiscal Year 2013 Budget Request for the Department of Homeland Security*, March 21, 2012. Available at: <http://www.dhs.gov/news/2012/03/21/written-testimony-dhs-secretary-janet-napolitano-senate-committee-homeland-security> (accessed February 21, 2015).
- U.S. DHS, Homeland Security Advisory Council, *Report of the Critical Infrastructure Taskforce*, January 2006. Available at: [http://www.dhs.gov/xlibrary/assets/HSAC\\_CITE\\_Report\\_v2.pdf](http://www.dhs.gov/xlibrary/assets/HSAC_CITE_Report_v2.pdf) (accessed February 21, 2015).
- U.S. DHS, Transportation Security Administration, *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*, May 2007, p. 1. Available at: <http://www.hsdl.org/?view&did=474328> (accessed February 21, 2015).
- U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection: An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts Across Ports and Other Infrastructure* (GAO-13-11), October 25, 2012. Available at: <http://www.gao.gov/products/GAO-13-11> (accessed February 21, 2015).
- U.S. GAO, *Critical Infrastructure Protection: DHS List of Priority Assets Needs to be Validated and Reported to Congress* (Washington, DC: U.S. GAO, 2013).
- R.H. Ullman, "Redefining Security," *International Security*, 8(1) (1983): 129–153.
- S.M. Waltz, "The Renaissance of Security Studies," *International Studies Quarterly*, 35 (1991): 211–239.
- K.N. Waltz, *Theory of International Politics*. Reading, MA: Addison-Wesley, 1979.
- K.N. Waltz, "The Emerging Structure of International Politics," *International Security*, 18 (1993): 44–79.
- B. Weiser and A. Baker, "A Bridge Under Scrutiny, by Plotters and the Police," *The New York Times*, April 26, 2011.
- White House, *U.S. National Security Strategy*. Washington, DC: White House, 2010, p. 1.
- E.B. Williamson and D.G. Winget, "Risk Management and Design of Critical Bridges for Terrorist Attacks," *ASCE Journal of Bridge Engineering*, 10 (2005): 96–106.
- B. Zhu, A. Joseph, and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in *Internet of Things (iThings/CPSCom), 2011 International Conference/fourth International Conference on Cyber, Physical and Social Computing*. New York: IEEE, 2011, pp. 380–388.

---

# 5

---

## TRAVELERS' PERCEPTIONS OF SECURITY FOR LONG-DISTANCE TRAVEL: AN EXPLORATORY ITALIAN STUDY

EVA VALERI<sup>1,2,\*</sup>, AMANDA STATHOPOULOS<sup>3</sup>, AND EDOARDO MARCUCCI<sup>4</sup>

<sup>1</sup>*European Commission, Joint Research Centre (JRC), Institute for Prospective Technological Studies (IPTS) Edificio Expo, c/Inca Garcilaso, Seville, Spain*

<sup>2</sup>*DEAMS, University of Trieste, Trieste, Italy*

<sup>3</sup>*McCormick School of Engineering & Applied Science, Northwestern University, Evanston, IL, USA*

<sup>4</sup>*DISP, CREI, University of Roma Tre, Rome, Italy*

### 5.1 INTRODUCTION

Passengers' security ranks high on the political agenda especially when it comes to the aviation sector. However, recent international terrorist attacks on rail systems, as well as the limited entry and exit points to these systems, have directed some attention to rail security too. Over the past decade, security concerns have increasingly focused on rail passengers due to terrorist bombings within rail stations and rail cars in several major cities.<sup>1</sup> Furthermore, significant work has been undertaken to promote security

\*The views expressed are purely those of the author and may not in any circumstances be regarded as stating an official position of the European Commission.

<sup>1</sup>Amtrak (2010). Amtrak security efforts aim to defeat and deter most dangerous and likely terror tactics. National Railroad Passenger Corporation (Amtrak), New Release. Available at [http://www.amtrak.com/ccurl/7/679/ATK-10-051%20Amtrak%20Security%20Efforts%20Aim%20to%20Defeat%20and%20Deter%20\(04-21-10\).pdf](http://www.amtrak.com/ccurl/7/679/ATK-10-051%20Amtrak%20Security%20Efforts%20Aim%20to%20Defeat%20and%20Deter%20(04-21-10).pdf).

requirements in the railway sector across Europe. The rail network has a European dimension, while high-speed rail (HSR) is a potentially attractive target for terrorist acts. In fact, national HSR networks are usually considered a national symbol. Terrorist attacks have long been acknowledged as having significant impacts on travel behavior (Edmonds and Mak 2006; Hall 2002). Security, in fact, is not a positive selling feature that attracts customers or passenger for much of the transport sector (European Commission 2012). The most influential event worldwide, under this respect, in the near past has surely been the terrorist attacks in the United States on September 11, 2001. This single event has had an enormous impact on international and domestic travel patterns. In fact, not only did the events affect decisions regarding where to travel, but they also impacted on choices regarding mode of transport and, in some cases, whether to travel at all (Hall 2002). The events raised broader questions about the overall security of travelers from terrorist or criminal acts. These issues have long been acknowledged as relevant in influencing tourist decision making (Hall and O'Sullivan 1996), but following terrorist attacks targeting public transport systems worldwide, security has become a top priority in the policy agenda for all the transport sectors. Terrorist groups, thanks to their ease of access and vulnerability, have targeted these open networks. Terrorists are well aware that the widespread use of transportation under the fear of terrorist attack has the potential to cause mass panic, disruption, and fear (Potoglou et al. 2010). Security measures should provide users with a sense of confidence when using the transportation system at any time. In order to ensure security within the EU, it may be necessary to implement transport security-related actions outside the EU before a journey to the EU commences (European Commission 2012). No sufficient effort to prevent terrorist attacks has been made. This phenomenon is evolving over time. It has specific characteristics in each country. Probably, there will never be a complete level of security, and it may not be desirable to even seek it. Appropriate international and national security policies should explicitly consider travelers' perceptions and attitudes since these are critical elements in choosing whether to travel (or not) or the type of transport mode use.

The iJET International (2012) provided assessments of security risks faced by travelers (on a five-point scale, ranging from 1, less risky, to 5, more risky), using more than 190 countries as a reference. From this study, we can observe an overall stability in the synthetic security risk index for Italy in the 2004–2011 period (with a constant score of 0.75 for each year).<sup>2</sup> Unfortunately, no data are provided after the critical year of 2011. However, a general and slight increase of security risks might reasonably be assumed. The Foreign and Commonwealth Office (2012)<sup>3</sup> of the UK government provides travelers, based on survey results, country information on security issues, which for Italy can be summarized as follows: *There is a general threat from terrorism. [...]. On 11 December 2012 home-made bombs were found outside*

<sup>2</sup>iJET uses its predictive intelligence model to assess and rate the security levels of hundreds of countries and cities. This model helps to take informed decisions that protect people, facilities, and assets better. The Italian synthetic security risk index was stable at 0.75 for every year from 2004 to 2011.

<sup>3</sup><http://www.fco.gov.uk/en/travel-and-living-abroad/travel-advice-by-country/europe/italy>

*two banks in the centre of Rome and at a bank in Genzano, [...]. In May 2012, an explosion outside a school in Brindisi caused fatalities and injuries [...]. In December 2010, parcel bombs exploded in the Swiss and Chilean embassies in Rome, [...]. Also in December 2010, a parcel bomb was found at the Greek Embassy in Rome, [...].*

The paper provides preliminary evidence from an Italian case study focusing on the perception of security risk associated with different modes for long-distance travel. In particular, our paper investigates (i) the impact security issues have on travel behavior and mode choice for long-distance travel and (ii) the travelers' perception for government's efforts to ensure high security to citizens. Segmentation analyses based on socioeconomic characteristics of respondents were carried out in order to identify people strongly affected by the risk of terror attacks. Our results are based on an ad hoc survey administered in Rome during May 2011.

In Section 5.2, a synthetic literature review is reported. The methodological approach is illustrated in Section 5.3. Section 5.4 describes the survey features in detail and reports the results. Section 5.5 provides final remarks and future research.

## 5.2 LITERATURE REVIEW

Research conducted in the transport sector analyzing the impact of security focuses on threats originating from outside the transportation system itself. As mentioned earlier, public transportation risks typically receive more attention than risks associated with private mobility due to their high profile and targeted media coverage. Despite the relevance of real and perceived risks associated with using public transport, there are several issues that warrant attention in the literature. This review will explore the impact of real and perceived security and how this influences both traveler's propensity to use different transport modes and traveler's perception about government's efforts to ensure high security to citizens. To do this, we selected the most relevant papers from the literature.

There is growing evidence that passengers are discerning a lack of security while using public transportation, which is, as of yet, ill understood by analysts (Paulley et al. 2006). Conducting 20 focus groups and a large-scale Internet survey of 2000 respondents, a recent research carried out in the United Kingdom by Stevens and Vaughan-Williams (2012) found that individuals identify threats at multiple levels (global, national, community, family, and individual) and that while these threats are related, they are also distinct.<sup>4</sup> Moreover, some of the determinants of threats' perceptions are common,<sup>5</sup> but there was also systematic variation.<sup>6</sup> In fact, systematic variation was found in how different levels of threat affect political attitudes, behavior, and policy preferences. Their findings show a disparity between what the government considers to be the most pressing

<sup>4</sup>For instance, on average, individuals identify more threats to the globe than to their communities.

<sup>5</sup>For instance, mortality salience and news consumption

<sup>6</sup>For instance, authoritarians identify more threats at the national, community, and personal/family levels, but they found no evidence of an effect on perceptions of global threats.

security threats facing the United Kingdom and what the public perceive as the most threatening. They found that despite government initiatives (including a “Big Society” approach) to the involvement of citizens in national security architectures, the British public was not aware of security policy.<sup>7</sup> However, there is no evidence to support the view that the small minority who are aware of the National Security Strategy are any “less” likely to perceive security threats across all four levels. Finally, while perceptions of threats at the national level are connected with policy preferences for enhanced security measures as solutions (e.g., tougher border security), threats perceived globally appear to be linked to less traditionally security-oriented policies such as international aid (Stevens and Vaughan-Williams 2012). Daly et al. (2011) focus on the role of user attitudes in determining the behavioral impact of security measures and security benefits obtained, using a more sophisticated approach. Taken together, such pioneer empirical studies considering the links between security/safety and surface transit behavior provide some preliminary indications on the important roles of user perceptions, past experience, agreement with security measure’s aims, and design and privacy concerns. In particular, estimating a latent variable choice model with ordered attitudinal indicators, they found that individuals concerned about their privacy would be less in favor of this type of security check than the rest of the sample. Moreover, they highlighted that the valuation of specific types of security check (e.g., metal detectors and X-rays) was influenced by attitudes for concern for privacy, security, and liberty. Moreover, people with high concern place a lower value on the introduction of X-ray check or metal detectors for rail travel. In fact, respondents who are more concerned about security, privacy, and liberty will be less likely to agree with the notion that every traveler should be checked.

Understanding the links between mode utilization and different types of risks is needed to promote socially beneficial mode shifts. Surveys from an air travel context show that views regarding security levels can play an important role in passenger mode choices, in understanding the role of security perceptions on intercity travel decisions (Srinivasan et al. 2006).

Srinivasan et al. (2006) found that individuals who hold positive impressions about the security measures are more likely to fly, but at the same time, the benefit obtained using the air mode decreases with increasing inspection and boarding time. Their results implied that the Transportation Security Administration should both improve the public perceptions of the security arrangements and ensure fast and efficient screening so as to sustain the air travel demand.

The literature has moreover explored how different types of users react. A British study indicates that the amount of public transportation trips could rise by 10% if passengers felt more secure (Crime Concern 2002). Smith (2008) describes the role of women in public transport, underscoring the strong impact of security shortcomings on the trip timing, suppression, and choice of travel mode. Based on data from the Chicago Transit Authority Customer Satisfaction Survey of 2003, Yavuz and

<sup>7</sup>In fact, only 11% of surveyed respondents were aware of the UK National Security Strategy.

Welch (2010) find that train transit security affects men and women differently. For instance, the presence of video cameras as a security measure has a weaker effect on women's feelings of security compared to that of men. The use of surveillance and security measures generally contributes toward the public's perceptions of security. In this context, however, there are important trade-offs to consider, since an accentuation of security measures may lead to privacy invasion and impediments of passenger's free movement. Control measures perceived as too cumbersome or invasive may not be acceptable to users and lead to an exodus of travelers toward other transport modes. Findings from an intercity business traveler survey indicated that respondents who agreed more with the security measures were more willing to accept security-derived delays and tended to keep traveling by air (Srinivasan et al. 2006). Elias et al. (2013) study the effects of terrorist threats on refraining from traveling by bus and the extent of passengers' fear and risk perception of a terrorist attack for surface transportation. Collecting 662 interviews in Jerusalem and Haifa (Israel) during October 2009, they found the following: (i) in both cities, women are significantly more afraid than men of a terrorist attack in all public transportation modes tested (bus, train, and car), as well as of being involved in a road crash; (ii) the population sample in both cities is more afraid of a terrorist attack on buses, especially intracity buses, than on trains; and (iii) with reference to the comparison between the extent of the fear of terrorist attacks and the fear of being involved in a road crash, the second one is notably higher in both cities. Furthermore, their results show that 6.6% of the respondents from Haifa and 10.3% of the respondents from Jerusalem answered that they themselves (or a close family member) had been wounded in a terror attack. Moreover, in case of refraining from bus use, they found that the favored transport mode is a passenger car (and if this mode is not available at all, taxi option is the preferred mode).

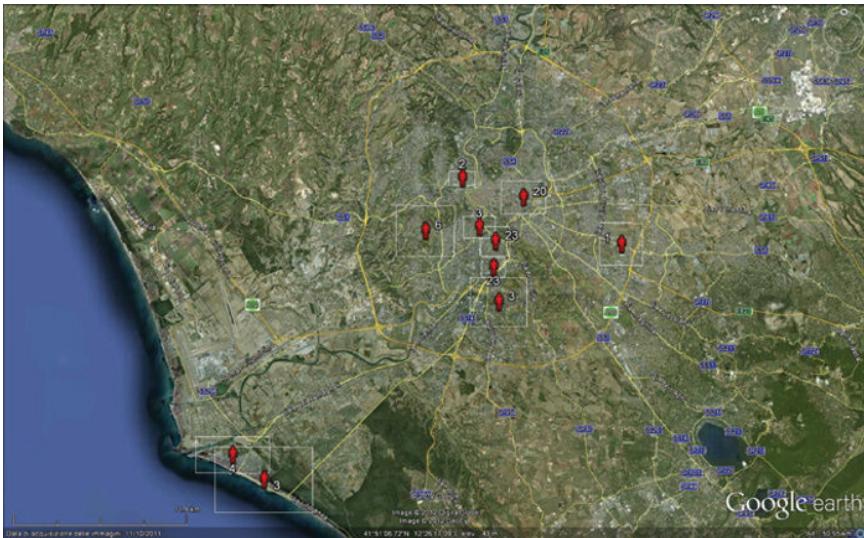
Despite a growing attention in the transportation literature to the impact of security on travel behavior, the focus is mainly on local or urban transportation behavior. Instead, there is a lack of studies in the area of long-distance traveling. The current work aims to provide some preliminary evidence, from an Italian context, concerning the risk perception associated with different mode options for long-distance trips. By controlling also for past behavior and perceptions, it is possible to draw some first conclusions concerning the role of security threats on travel choices.

### 5.3 METHODOLOGY

The methodology is based on questionnaires administered in the city of Rome (Italy). Rome, which is located in the center of the peninsula, is the largest city (with 3,997,465 inhabitants in 2011<sup>8</sup>), and it is also the main Italian railway node. There are five railway stations. The main stations are Rome Termini and Rome Tiburtina,<sup>9</sup> where HSRs operate daily since 2009 to connect north, south, and east of Italy. There

<sup>8</sup>[http://dati.istat.it/Index.aspx?DataSetCode=DCIS\\_POPSTRRES1&Lang=IT](http://dati.istat.it/Index.aspx?DataSetCode=DCIS_POPSTRRES1&Lang=IT)

<sup>9</sup>Other rail stations in Rome are Roma Trastevere, Roma Tuscolana, Roma Ostiense, and Roma San Pietro.



**FIGURE 5.1** Map of respondents (Source: Our elaboration with Google Earth).

are also two airports, the international Rome Fiumicino airport and the city airport Rome Ciampino. Rome is the main starting point for medium- and long-distance travels. These reasons motivate our choice of Rome as a focus of research.

In each location (Fig. 5.1), we have only interviewed those people who have traveled or were traveling for a long-distance trip<sup>10</sup> departing or returning from Rome. Individuals were approached and interviewed only if at least the origin (or destination) of the last/current trip was Rome. Interviewers performed a paper-and-pencil interview. A later stage of data entry was needed.

The questionnaire is composed of four parts aiming at the collection of data concerning:

1. Socioeconomic and demographic characteristics of respondents (e.g., age, gender, education, employment, residence, income, etc.)
2. Revealed preference data on the last/current long-distance trip and their travel behavior in relation to hypothetical changes in security
3. Respondents' attitudes and perceptions about government effort to prevent terrorist attacks
4. Respondents' comments provided during the interview process and gathered by the interviewers

<sup>10</sup>There is not a common accepted definition of long-distance travel due to its complexity (for instance, it depends of the type of mode, type of mobility, type of travel's purpose, country's features, the methodology used to calculate it, etc.) (Axhausen 2001; Bricka 2001; Dargay and Clark 2012; Madre and Maffre 2001). However, NTS Communications provides relevant data about the definition of long-distance travel by comparing many European countries. For a synthetic overview, see Kuhnlimhof (2007). We considered a long-distance (or intercity) trip travels for over 400 km.

Five trained and experienced interviewers administered the questionnaires.<sup>11</sup> For each administered interview, the interviewers made a detailed summary on respondent's behavior and comments during the interview process (questionnaire section number 4).<sup>12</sup>

## 5.4 THE ITALIAN CASE STUDY

This section describes the ad hoc survey and presents its results. The survey focuses on (i) the impact security issues have on travel behavior and mode choice for long-distance travel and (ii) the travelers' perception for government's efforts to ensure high security to citizens.

### 5.4.1 Survey Description and Design

Italian respondents were interviewed in Rome during May 2011. The locations chosen to hold the interviews were selected according to two main principles: (i) areas of Rome with high population concentrations (with a wide spectrum of the population) and (ii) transport- and nontransport-related places.<sup>13</sup> At each location, the sample was stratified by age and gender. The questionnaire was first tested using a pilot study that involved both academic staff and researchers at the University of Roma Tre. The questionnaire is a mix of closed- and open-ended questions. A total of 100 respondents completed the interview. Their location in Rome is reported in Figure 5.1 showing a concentration of the respondents in the city center.

### 5.4.2 Sample and Travel Behavior Features

Table 5.1 reports an overview of the sample characteristics. The sample consists of 48% men and 52% women. Age ranges from 15 to 86 years with a mean of 36. Fifty-three percent of respondents hold a high school diploma and 41% a degree/postdoc. Most respondents are employees (34%) and students/student-workers (35%), indicating oversampling of this last category.

Fifty-five percent of the sample declares a monthly income of less than 1.500€, and 62% of respondents travel in a group, while 36% travel alone. Table 5.2 reports frequency of use for the two transport modes considered, revealing rail to be used more frequently than air transport.

<sup>11</sup>These undergraduate students attended an intensive seminar for applied economics course at the University of Roma Tre (Marcucci et al. 2011). The applied part of the course consisted in the questionnaire administration.

<sup>12</sup>For instance, it was detected if the respondent was attentive and interested—or careless and disinterested—during the interview. This type of data can be useful in the data cleaning process. Moreover, it allowed us to identify important aspects not directly detectable by the questionnaire and useful to explore this delicate and complex topic.

<sup>13</sup>Overall, interviews were carried out in the following places: underground/metro (24%); rail station (22%); open public places, Piazza del Popolo, Piazza Ottaviani, Colosseo, and Circo Massimo (22%); airports (12%), and enclosed public places, restaurants, banks, beauticians, universities, etc. (20%).

TABLE 5.1 Overview of Socioeconomic Data

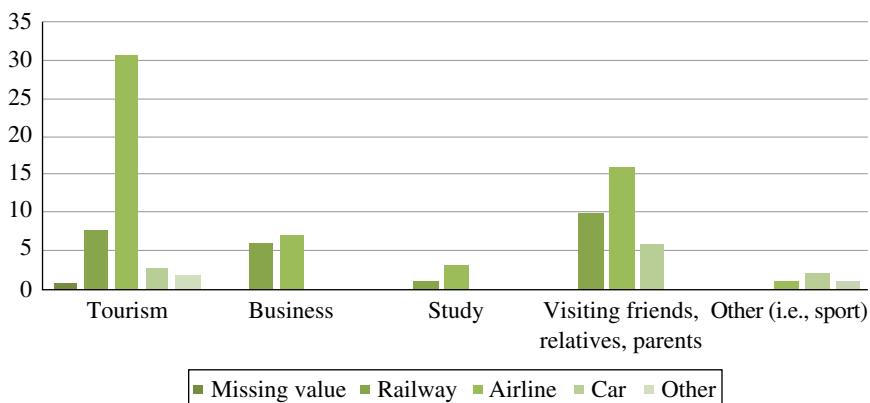
Gender	Age	Education	Employment	Income
Men	48%	15–85	Employee	34%
Female	52%	36 (average)	Manager	3%
Total	100%	High school Degree/postdoc Total	Freelancer Student Student-worker Retired Unemployed Others Total	<500€ 501–1,500€ 1,501–2,500€ 2,501–3,500€ 3,501–4,500€ >4,501€ Missing value Total 100%

Source: Our elaboration.

**TABLE 5.2 Frequency of Transport Mode Use**

	Frequency of use (%)						Total
	Once or more times a week	Once every two weeks	Once or more times a month	Once or more times a year	Never	Missing value	
Air transport	0	0	12	79	8	1	100
Rail transport	10	3	17	55	14	1	100

Source: Our elaboration.



**FIGURE 5.2** Last/current long-distance travel—interaction between mode used and purpose (Source: Our elaboration).

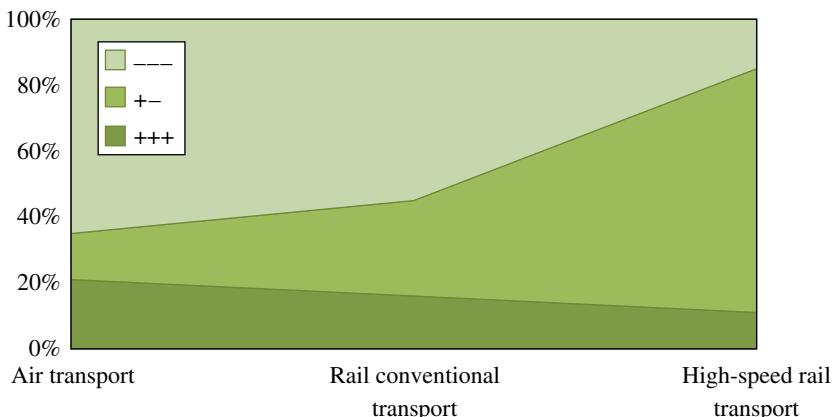
### 5.4.3 Description of the Last/Current Long-Distance Trip

A description of a representative long-distance trip is collected with the questionnaire. Figure 5.6 reports a geographic overview of all origins/destinations described by the respondents.

Forty-three percent of interviewees traveled in Italy, while 57% went abroad. Eighty-seven percent of interviewees referred their description to their most recent trip, while 13% described the current one.

Respondents traveled mainly for tourism (45%) and visiting parents, relatives, and friends (32%). A limited number of travels were made for business (4%) and study (4%) purposes (Fig. 5.2). Moreover, we asked the transport mode used for the last/current long-distance trip<sup>14</sup>: air transport is used by 58% of the sample, followed by rail (25%). For “other” purposes (e.g., sport), car is the most common mode, responding to special needs of such trips (e.g., flexibility) (Fig. 5.3).

<sup>14</sup>The available transport options were train, airplane, car, and ship.



**FIGURE 5.3** Respondents' perceptions of the security level of transport modes (Source: Our elaboration). Security levels are represented by the following Likert scale ----/+-/+++.

#### 5.4.4 Behavioral Travel and Mode Choice Patterns and Security Changes

In the section number 2 of the questionnaire, we collected data on the impact security issues have on travel behavior and mode choice for long-distance travel.

Regarding travel behavior, we asked the following question related to the last/current long-distance travel: "If a general increase in antiterrorism alert have occurred in your last/current long-distance travel, would you have made the journey anyway?" In particular, respondents were asked whether a general increase in antiterrorism alert would dissuade them from making the journey.<sup>15</sup> Fifteen percent of interviewees responded that they would have chosen to suppress the travel. This result highlights a nonnegligible portion of respondents who would have renounced to travel. A segmentation analysis based on socioeconomic features was carried out. The average profile of the respondent who gave up traveling is characterized as follows: 65 years old, female, traveling alone and for a business purpose, with a low

<sup>15</sup>This question was posed without describing the type of changing security, because this survey aims to explore the security issue. Moreover, terrorism does not have a single and accepted definition (for a brief history, see <http://en.wikipedia.org/wiki/Terrorism>, section "Definition"). In the questionnaire, terrorist attack was described as criminal acts intended or calculated to provoke a state of terror in the general public, institution, and/or authorities for political purposes through various activities (e.g., bombings, murders, massacres, kidnappings, sabotage, etc.). Obviously, in the next survey, the security concept will be further explored, separately analyzing, for instance, the different types of terrorism (e.g., civil disorder, political terrorism, nonpolitical terrorism, quasiterrorism, limited political terrorism, and state terrorism—for their description, see <http://en.wikipedia.org/wiki/Terrorism>, section "Types of terrorism").

level of education, mainly unemployed and freelance, and with an average monthly income less than 1.500€.

Regarding the travel mode choice, we asked the following questions related to a long-distance travel:

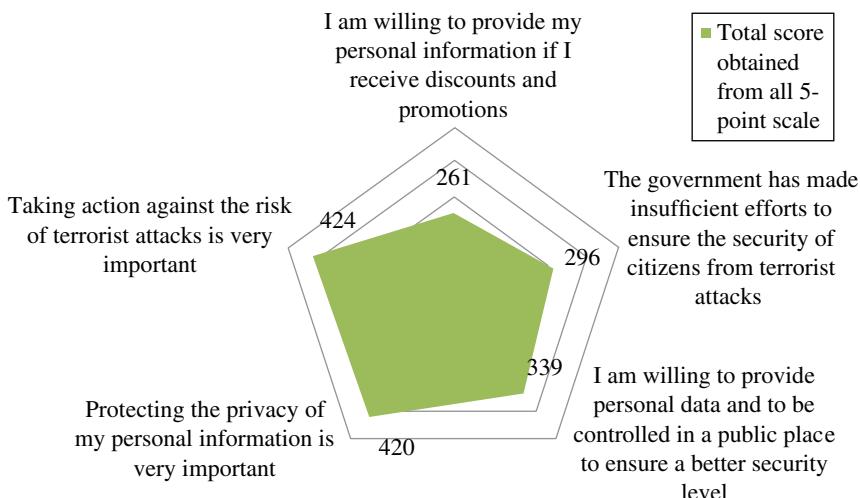
- (Q1) “Did you happen to renounce to travel with the planned transport mode for fear of a terrorist attack?” If the answer was “yes,” answer also the following two questions:
  - (1.1) With which transport mode would you have had to travel?
  - (1.2) With which transport mode have you decided to travel?
- (Q2) “What transport mode do you consider more secure from possible terrorist attacks?”

These questions related with revealed behavior of respondents. With reference to Q1, the results show that the 95% of the sample has never given up their planned long-distance transport mode due to a fear of a terrorist attack. Conversely, the remaining 5% decided to change their planned transport mode. While 60%<sup>16</sup> had originally planned to travel by air and 40%<sup>17</sup> by rail, they finally resorted to travel using a different mode. In particular, those who traveled with rail transport shifted to car and air transport. Moreover, the “not travel” option was only proposed by respondents who traveled by plane. This is due mainly to the difference of the traveled distance of the air transport mode with respect to the rail option. In fact, for rail passengers, car and airplane are possible substitute, while air passengers prefer renounce of their own travel. The average profile of the respondent who changed their planned transport mode is characterized as follows: aged between 35 and 66 years old, female, traveling alone and for leisure and business purposes, with a high level of education, mainly manager and freelance, and with a medium–high monthly income.

The questionnaire also aimed at seizing travelers’ perceptions of security levels when using different transport modes for long-distance travel (Q2). For this specific purpose, we preferred distinguishing between HSR and conventional low-speed rail given their different appeal as terroristic targets. Results are reported in Figure 5.4. The air transport is considered to be the most secure mode for 21% of the interviewers and contemporarily the least secure mode for 65% of them. In fact, the responses were polarized at the two extremes of the three-point scale. Also, conventional train is perceived to be rather unsafe by a large proportion of respondents (55%), while HSRs gained more responses in the “quite safe” (+-) level, corresponding to 74% of the cases, and a good score of the “very safe” (+++) level with a frequency of (11%). However, if we only consider the +++, air transport wins, but if we also consider +-+, fast-speed train is perceived as the safest mode.

<sup>16</sup>Sixty percent corresponds to 3 respondents.

<sup>17</sup>Forty percent corresponds to 2 respondents.



**FIGURE 5.4** Respondents' perceptions and attitudes toward security issues (average score for all five-point scale) (*Source*: Our elaboration). Scores were assigned by five-point Likert scale.

#### 5.4.5 Government Enforcement, Privacy, and Security Efforts

This section uses a five-point scale to identify whether people agree with or are aware of government's attempts to make travelers feel secure. Furthermore, this section reports the evaluations of these attempts, including an analysis of travelers' attitudes regarding privacy and security issues.

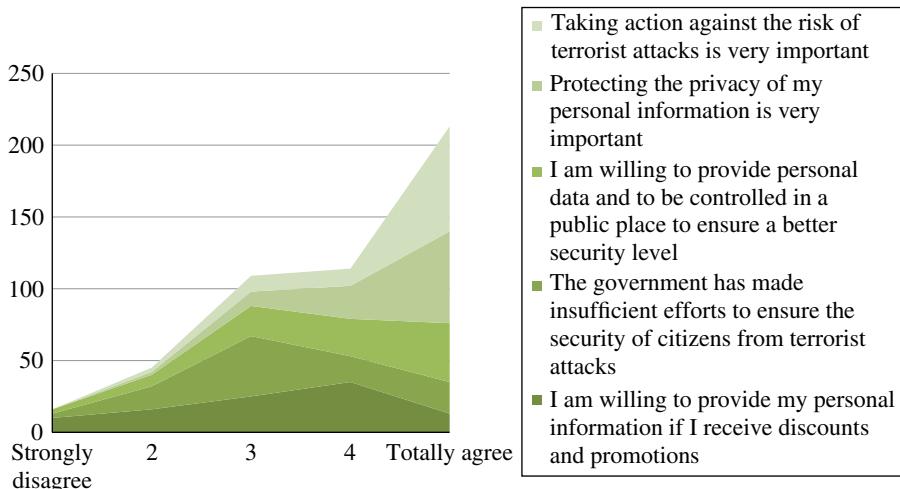
Figure 5.5 shows the total score obtained by each perception and attitude tested in the questionnaire defined as the sum of responses received from all five-point items across all respondents. Figure 5.6, instead, reports the scores of Figure 5.5, specifying its values for each of the five-point scale. The main findings are discussed in the following.

The majority of respondents acknowledged the importance of taking action against terrorist attacks (73%). Forty-one percent of the interviewees are ready to provide personal data and be controlled in exchange of higher levels of security notwithstanding that personal data is a key concern for many respondents (64%). Only 13% of the sample is willing to provide personal data for discounts and promotions.

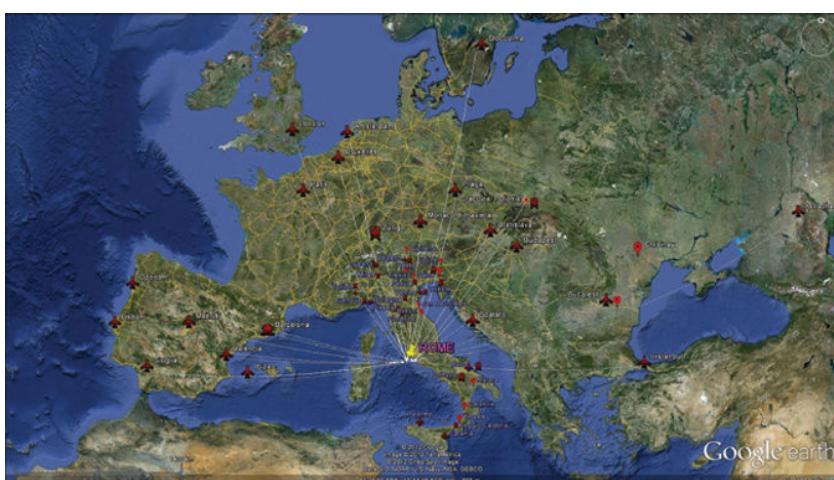
Figure 5.5 clarifies that government's efforts were assigned one of the lowest total scores (# 296). However, as shown in Figure 5.6, scores are concentrated around the central value of the five-point scale (# 3). Respondents, on average, indicated that government's effort is medium insufficient to ensure a high level of security.

A segmentation analysis of travelers' attitude and perception of government's efforts to ensure high security to citizens was performed, and its results are summarized below:

- Females perceive government's efforts as more insufficient with respect to males.



**FIGURE 5.5** Respondents' perceptions and attitudes toward security issues (score for each five-point scale) (Source: Our elaboration).



**FIGURE 5.6** Overview of the last/current long-distance travel (Source: Our elaboration with Google Earth).

- Respondents under 50 years consider government's efforts more insufficient than those above 50.
- Respondents with a higher net monthly income perceive government's efforts positively; on the contrary, respondents with a lower net monthly income spread their scores over all the five-point Likert scale.
- Respondents who travel frequently (both by train and by plane) perceive the government's efforts as "medium insufficient."

- Respondents who made the last (or current) travel abroad consider government's efforts more insufficient than those who took a domestic trip. Therefore, those making longer trips (i.e., abroad) perceive a greater need for security with respect to shorter trips. In this case, current government's efforts are inadequate in particular for long-distance travels. This respondents' perception may be due to various aspects (e.g., traveled distance, mode of used transport). However, segmenting by type of transport mode used in the last/current long-distance travel,<sup>18</sup> we did not find differences in considering government's efforts more insufficient for abroad travels. In fact, respondents who traveled by rail and air transport agree with adequate government's efforts if they traveled in Italy, while they disagree if they traveled abroad.
- Respondents interviewed at the rail stations believe that the government performed an adequate commitment to prevent terrorist attacks, while those interviewed in open public places (e.g., Piazza del Popolo, Colosseo, Circo Massimo) mainly agree with insufficient government's efforts. This may also be due to the objective difficulty of ensuring a high security level in open public places that are open system with numerous access points to terrorists.
- Respondents who are not influenced in their travel choices from an increase in the security alarm believe that the government was already providing, on average, an adequate level of security.
- Respondents who have refused to travel with the planned transport mode believe that the government showed an inadequate commitment to prevent terrorist attacks.
- Respondents who feel that taking actions to curb the risk of terrorist attacks is important also considered that government's efforts in this domain are insufficient.
- Respondents willing to provide personal data and be controlled with the declared aim of increasing the level of security consider government's commitment to prevent terrorist attacks insufficient.

## 5.5 CONCLUSION

Terrorist attacks have long been acknowledged to cause significant impacts on travel behavior. This paper provides preliminary insights on travel behavior/mode choice in response to a general increase in antiterrorism alert and travelers' perception for government's efforts to ensure high security to citizens. For all these aspects, segmentation analyses based on socioeconomic characteristics of respondents were carried out. Moreover, our contribution is focused on long-distance travels, a topic underresearched in the extant literature.

First, as motivated in Section 5.3, our choice of Rome as a focus of research was representative to analyze transport security issues.

<sup>18</sup>In particular between rail and transport modes

With reference to the impact security issue on travel behavior and mode choice, the main findings show that fear and risk perception of respondents are crucial aspects. In fact, we found that a nonnegligible portion of sample would have chosen to suppress the travel. Moreover, respondents perceived security risks related to transport modes in different ways, and their opinions are heterogeneous. Air transport is perceived as the most secure mode (21%), but at the same time, it is considered also the least secure by 65% of the sample. HSR is considered the most secure mode by a minority, but if the medium responses are included, on average, it has the highest perception of security.

With reference to the travelers' perceptions about government's efforts in security-related activities, the results can be summarized as follows:

- Taking action against terrorist attacks is a priority for respondents (73%).
- Protecting the privacy of personal data is important for respondents (64%), but they are also willing to provide personal data and to be monitored for a better level of security (41%). They are less willing to provide personal data in order to receive discounts and promotions (13%).

Respondents consider that government's security efforts are, on average, insufficient. For all the aspects analyzed, segmentation analysis revealed gender differences (for women, the impact on their travel behavior is more intensive) and allowed us to identify the respondent's profile that is more affected by changes in a security level. These results could be very useful for both policy-makers and transport operators in order to raise awareness on this issue and increase the effectiveness of their policies and business strategies. Travelers' perceptions about government's efforts in security-related activities impact their travel choices. For instance, 65% of respondents perceived air transport as the least secure; airport operators and airlines could be interested to in-depth analyze respondents' profile and motivations in order to attract new customers. Furthermore, our results show that respondents willing to both provide personal data and be controlled with the declared aim of increasing the level of security consider government's commitment to prevent terrorist attacks insufficient. This type of people should better accept policies such as cameras with visual recognition (allowing identification of users), metal detectors, or X-rays.

Moreover, some aspects of this research could undergo further investigation with the aim of strengthening or disconfirming the obtained results. For instance, in the next survey, we will analyze separately all the types of security levels (e.g., global, national, individual, etc.) in understanding how these levels are perceived by respondents and their related impact on the daily life of respondents. Moreover, we will explore separately both the main types of terrorism (e.g., civil disorder and limited political terrorism) and the motivations related to the perceived security risks connected to both travel behavior and different transport modes. Valuable research in this direction is proposed by Elias et al. (2013). However, because of the lack of studies focused on Italy, this preliminary analysis could also provide helpful suggestions for planning and designing a *stated preference* survey to test hypothetical security policies in order to analyze acceptability and possible reactions of

long-distance travelers further motivated by the important development of the Italian HSR network. A valuable research in this direction is proposed by Daly et al. (2011).

## ACKNOWLEDGMENT

We thank Luca Carapellese, Riccardo Celeghini, Dario Chimenti, Melissa Pezzi, and Saturnino De Sousa Carlo for administering the interviews and participating at the seminar *Techniques of interviews administration: Theory and applications* at the University of Roma Tre in May 2011.

## REFERENCES

- Axhausen KW (2001) *Methodological research for a European survey of long-distance travel*. Paper presented at the TRB Conference on Personal Travel: The Long and Short of It, June 28–July 1, 1999 Washington, DC.
- Bricka S (2001) *Variations in long-distance travel*. Paper presented at the TRB Conference on Personal Travel: The Long and Short of It, June 28–July 1, 1999 Washington, DC.
- Crime Concern (2002) People Perceptions of Personal Security and Their Concerns about Crime on Public Transport: Literature review. Crime Concern for Department for Transport. Available at: [http://www.activcameras.com/downloads/dft\\_mobility\\_029301.pdf](http://www.activcameras.com/downloads/dft_mobility_029301.pdf) (accessed on March 10, 2015).
- Daly A, Hess S, Patruni B, Potoglou D, Rohr C (2011) Using ordered attitudinal indicators in a latent variable choice model: a study of the impact of security on rail travel behaviour. *Transportation*, 39 (2):267–297.
- Dargay JM, Clark S (2012) The determinants of long distance travel in Great Britain. *Transportation Research Part A: Policy and Practice* 46 (3):576–587.
- Edmonds C, Mak J (2006) *Terrorism and Tourism in the Asia Pacific Region: Is travel and Tourism in a New World After 9/11?* East-West Center Working Paper, Economic Series, February n. 86.
- Elias W, Albert G, Shiftan Y (2013) Travel behavior in the face of surface transportation terror threats. *Transport Policy* 28:114–122.
- European Commission (2012) Commission Staff Working Document on Transport Security. Brussels, 31.5.2012 SWD(2012) 143 final. European Commission, Brussels.
- Foreign and Commonwealth Office (2012) Travel advice to travel in Italy—Safety and security. Available at: <http://www.fco.gov.uk/en/travel-and-living-abroad/travel-advice-by-country/europe/italy> (accessed on March 10, 2015).
- Hall CM (2002) Travel safety, terrorism and the media: the significance of the issue-attention cycle. *Current Issues in Tourism* 5 (5):458–466.
- Hall CM, O'Sullivan V (1996) Tourism, political instability and violence. In: Mansfeld APaY (ed.) *Tourism, Crime and International Security Issues*. John Wiley, New York.
- iJET International (2012) Security assessment ratings. World Bank. Available at: [info.worldbank.org/governance/wgi/pdf/IJT.xlsx](http://info.worldbank.org/governance/wgi/pdf/IJT.xlsx) (accessed on March 10, 2015).
- Kuhnimhof T (2007) Long Distance Travel in Europe: Surveying Methods, Data Availability and Comparability (COST355). October 5 In Torino.

- Madre JL, Maffre J (2001) Is It Necessary to Collect Data on Daily Mobility and Long-Distance Travel in the Same Survey? Paper presented at the TRB Conference on Personal Travel: The Long and Short of It, June 28–July 1, 1999 Washington, DC.
- Marcucci E, Valeri E, Stathopoulos A (2011) Techniques of interviews administration: theory and applications. University of Roma Tre—integrative seminar for the degree course Applied Economics (Prof. E. Marcucci), 25 hours. Available at: [http://scienzepolitiche.uniroma3.it/files/2009/10/Sem\\_MAG\\_TRI\\_Marcucci.pdf](http://scienzepolitiche.uniroma3.it/files/2009/10/Sem_MAG_TRI_Marcucci.pdf) (accessed on March 10, 2015).
- Paulley N, Balcombe R, Mackett R, Titheridge H, Preston J, Wardman M, Shires J, White P (2006) The demand for public transport: The effects of fares, quality of service, income and car ownership. *Transport Policy* 13 (4):295–306.
- Potoglou D, Robinson N, Kim CW, Burge P, Warnes R (2010) Quantifying individuals' trade-offs between privacy, liberty and security: The case of rail travel in UK. *Transportation Research Part A: Policy and Practice* 44 (3):169–181.
- Smith MJ (2008) Addressing the security needs of women passengers on public transport. *Security Journal* 21:117–133.
- Srinivasan S, Bhat CR, Holguin-Veras J (2006) Empirical analysis of the impact of security perception on intercity mode choice. *Transportation Record* 1942:9–15.
- Stevens D, Vaughan-Williams N (2012) *Attitudes towards security threats uncovered*. Universities of Exeter and Warwick, Coventry, UK.
- Yavuz N, Welch E (2010) Addressing fear of crime in public space: Gender differences in reaction to safety measures in train transit. *Urban Studies* 47:2491–2515.



---

# 6

---

## SECURING TRANSPORTATION SYSTEMS FROM RADIOLOGICAL THREATS

ERIC P. RUBENSTEIN<sup>1</sup>, GORDON A. DRUKIER<sup>1</sup>,  
AND PETER ZIMMERMAN<sup>2</sup>

<sup>1</sup>*Image Insight, Inc., East Hartford, CT, USA*

<sup>2</sup>*King's College London, Arms Control Expert & Nuclear Physicist, London, UK*

### 6.1 THE THREAT

Radioactive substances are in many ways an ideal threat material. Invisible, odorless, and silent, the radiation they emit has the capacity to inflict injury on many people. When the right isotopes are used, even very small amounts—such as the size of a pea—can pose a mortal threat given sufficient exposure. Transportation systems are places where people congregate and often remain in confined areas for extended periods and could therefore be tempting targets for high-impact terrorist attacks using radiological sources. In this article, we will explain the threat environment in more detail and explain how radiation detection technologies can be used to give early warning of radiological threats and to mitigate their impact.

### 6.2 RADIATION SOURCES AND THEIR DETECTION

Electromagnetic radiation takes many forms, principally visible light and its lower- and higher-energy analogs. But in the context of threats to the health and security of passengers on transportation systems, the *ionizing radiation*

emitted by radioactive atoms poses the greatest threat and is the subject of this chapter.

Nearly all chemical elements have multiple isotopes—that is, chemically identical atoms of different atomic mass. Some isotopes are stable, while others are unstable and undergo radioactive decay events. In an attempt to achieve stability, one of several possible radioactive decays takes place, usually transforming the atom into an isotope of another element. This “daughter particle” may also be unstable, in which case further radioactive decay may be expected, or it may be stable, in which case no further decays occur. Most elements have naturally occurring radioactive isotopes, but these tend to be present in small proportions in natural materials. The isotopes of concern here are man-made and are in use in various settings including hospitals, industrial radiography, and the oil industry.

Radioactive decay takes three forms, emitting what were originally called alpha, beta, and gamma particles. We now know that alpha particles are nuclei of helium atoms: two protons plus two neutrons. Beta particles are either electrons or their anti-matter counterparts, called positrons. Gamma rays are high-energy electromagnetic radiation. The radiation from gamma-ray emitters falls into roughly the same part of the energy spectrum where, if not produced by an atom’s nucleus, they would be called X-rays.<sup>1</sup> Some alpha and beta emitters also produce gamma rays when they decay. Additionally, when very energetic alpha or beta particles hit other materials, they interact within a very short distance, often creating X-rays as they do so. The type and energy of the radiation emitted by a particular isotope is peculiar to it, and can be used for identification of the threat isotope, much as a fingerprint can be used to identify a person. Relatively thin layers of shielding material, including air, readily stop alpha and beta particles. It is the gamma rays that pose the greatest external threat.

The rate at which radioactive decays take place varies from isotope to isotope, with the timescale measured in terms of the “half-life,” the time required for half the atoms in a sample to undergo a radioactive decay. Half-lives range from tiny fractions of a second to billions of years.

The radiation field associated with a quantity of radioactive material drops off as the square of the distance. So, for any given source, the measured dose rate depends strongly on the distance to the source. Conversely, once radiation is detected, a given dose rate may indicate either a weak, nearby source or a stronger, more distant source. The danger posed by any particular isotope depends on both its half-life and the type and energy of the radiation it emits. Isotopes with a shorter half-life emit radiation more intensely than those with a longer half-life but are a threat for a shorter period of time. Thus, the isotopes of most concern are high-energy gamma-ray emitters with half-lives of a few years to a few tens of years. The United Nations International Atomic Energy Agency (IAEA) has developed a list of the most readily available isotopes that pose the greatest threat to public safety and gives guidance on managing such radioactive sources.<sup>2</sup> Of these isotopes, cobalt-60 (half-life of 5.3 years)

<sup>1</sup>In other words, once produced, there is no difference between X-rays and gamma rays.

<sup>2</sup>The IAEA’s “Code of Conduct” and several related documents can be found at <http://www-ns.iaea.org/tech-areas/radiation-safety/code-of-conduct.asp>.

and cesium-137 (half-life of 30.2 years) pose the greatest threat from the standpoint of availability combined with radioactivity. Much attention is placed on managing gamma-radiation sources due to their frequent use in medical and industrial applications and the potentially lethal exposure levels that can be generated from purely external irradiation. Since these sources are not always adequately protected, authorities in charge of securing transportation systems need to be aware of the illicit or improper transportation of radiological materials through, or to, transportation facilities and vehicles.

Another type of ionizing radiation is in the form of neutrons, which are produced mostly by a few high-mass isotopes that undergo radioactive decay by spontaneous fission. Although the somewhat common element thorium produces a small amount of neutrons, they are more typically encountered emanating from uranium and plutonium, two elements rarely found outside of the highly controlled nuclear power and nuclear weapon industries. Neutrons can also be produced by combining an alpha-emitting isotope with a low-mass isotope that has a high probability of absorbing the alpha particle and emitting a neutron as a by-product of the transmutation. Neutrons on their own can penetrate some distance, but are readily absorbed by many materials including water. Besides causing direct damage, neutrons can also fuse with atomic nuclei, transforming them into other isotopes, oftentimes radioactive themselves. As a result of this “neutron activation,” alpha, beta, or gamma radiation will be released *in situ*. Neutron detection in the homeland security arena is usually focused on the detection of nuclear weapons and improvised nuclear weapons, although nuclear power fuel and spent fuel must also be accounted for.

There are a large variety of technologies used for radiation detection. In deciding which technology to employ for a particular application, the trade-offs are between capabilities and limitations. For radiation detection, the issues are, on the one hand, sensitivity, precision, and energy discrimination and, on the other hand, fragility, stability, availability, and, of course, cost. No matter the technology, radioactive decay is a random process, so the radiation level varies from measurement to measurement. Devices with higher sensitivities will give a reading to a given precision faster than those with lower sensitivity. At high radiation levels, speed is less of an issue, but some technologies saturate at high levels and provide little quantitative guidance. Under some circumstances, it is desirable to know not only if radiation is present but the type of radiation and the emitting material. For these purposes, there is a need to employ a technology that can measure the energy of the radiation, especially that of the penetrating gamma rays, and from that information deduce the identity of the radiating material.

Radiation detectors fall into three broad classes: gas detectors, semiconductor detectors, and scintillator detectors. A comparison of the various types of detectors for alpha, beta, and gamma radiation is given in Table 6.1.

The most common gas-based detector is the Geiger–Müller (G–M) detector. With these, a high voltage is applied across a tube filled with a low-density gas. When ionizing radiation enters the tube, the electrically neutral gas becomes ionized. The ions move toward the cathode and the electrons to the anode. Collisions along the way lead to additional ionization, a cascade of charge generation, and a brief pulse of

**TABLE 6.1 Comparison of Radiation Detector Properties**

Detector	Sensitivity	Energy Resolution	Cost	Availability	Comments
Geiger–Müller Proportional counter	Low Low	N/A Moderate	Very low Low	High High	Only operates as a counter Useful only for alpha, beta, and low-energy gamma rays
<i>Semiconductor Detectors</i>					
CdTe	Medium	1–2%	High	Satisfactory	Limited device size
CZT	Medium	1–2%	High	Low	Limited suppliers
HgI <sub>2</sub>	High	1%	High	Limited	One supplier
Ge	High	0.5%	Very high	High	Cooling required
CCD/CMOS digital camera based	Very low	Low	Very low	Very high	Can be used for radiation detection in parallel with standard CCTV surveillance network
<i>Scintillator Detectors</i>					
CsI(Na), CsI(Tl)	Medium	6%	Low	High	Mildly hygroscopic
NaI(Tl)	Medium	6%	Low	High	Hygroscopic
LSO, LGSO, LYSO, etc.	High	10%	High	Available	Self-activity
BGO	High	9% 6–8%	High	Available	Nonhygroscopic
CdWO <sub>4</sub>	High	—	High	Limited	Nonhygroscopic
Plastic scintillator	Low	— None	Low	High	No gamma–neutron discrimination Not suited for small gamma-ray detectors

current. These can be reported as the classic audible clicks, but modern G–M counters count the pulses digitally. After each pulse, there is a period of dead time while the charge disperses. G–M tubes can be fragile, require batteries, and, in active use, need to be replaced every few years. Similar concepts underlie the proportional counter and ionization chamber, but these are used more in the laboratory setting than in the field due to their inherent fragility.

Scintillator-based detectors use special materials that emit a pulse of light when it interacts with ionizing radiation. Highly sensitive, and often delicate, electronics pick up this faint light and process the signal into a measurement for the operator. Scintillator materials come in two varieties: crystals and plastic. Photomultiplier tubes examine the block of scintillator and collect the light produced by the radiation. The size and shape of individual pulses give information on the energy of the incident radiation. Unlike the other technologies, some scintillators are also sensitive to neutrons. Crystal scintillators can be fragile and expensive, and some are hygroscopic, meaning that they must be sealed against moisture to function properly.

Scintillators require the use of a photosensor to detect the optical light signal generated. The photomultiplier tubes that are traditionally used for this purpose cost several hundred dollars, are somewhat heavy and fragile, and require about 1000V to operate. Avalanche photodiodes are an alternative solid-state device with comparable performance, and they are substantially less expensive; they also require high voltage. Scintillator crystals can be coupled to less expensive readout devices, such as photodiodes or CCDs, but can then only be used as radiation counters, since no useful energy resolution is obtained from a scintillator when used in this way.

In semiconductor detectors, ionizing radiation traversing the material produces a pulse of current. In this case, the gamma-ray energy is directly changed into electric charge and, as a result, can provide better energy resolution than other technologies. The limitation is that it is generally easier to collect light from a scintillator than charge from a semiconductor, which limits the useful size of semiconductor sensors, and thus their overall sensitivity. The detectors operate at room temperature and provide reasonably good energy resolution. They are significantly more expensive than scintillators and are generally available in relatively small sizes only.

A low-cost solution is to harness commercially available CCD or CMOS cameras, which are now ubiquitously distributed in surveillance applications and handheld devices. In these devices, the energy deposited by ionizing radiation appears as abnormally bright pixels within the video or still images produced by these cameras. Counterintuitively, cameras can detect ionizing radiation from any direction since the lens does not focus the gamma rays, which instead penetrate the camera body. Although sensitivity is maximized when no optical light reaches the camera chip, this technology has been tested and deployed in normal transit security applications where the cameras are used normally (Rubenstein and Drukier 2009). Of the two common technologies, CMOS cameras tend to be about 10 times more sensitive than similarly sized CCD cameras. While the efficiency of the imagers is much lower than the other options and their energy resolution limited, they are very low cost both to procure and install. Utilization of existing security infrastructure further reduces these costs. The result is the potential for a broad network of inexpensive radiation detectors.

Table 6.2 shows a selection of neutron detector materials. The light helium isotope,  $^3\text{He}$ , is an obvious choice for a neutron detector, but the lack of an adequate and reliable supply of  $^3\text{He}$  removes this from consideration. Plastic scintillators are inexpensive and useful for detection of high-energy neutrons. Discrimination of neutrons from gamma rays is an issue for the scintillator-based neutron detectors, which also share the other limitations of scintillator detectors discussed previously.

The units used for measuring radiation are a confusing jumble. In addition to the distinction between the SI units and the non-SI units commonly used in the United States, we must also distinguish between units for radioactivity, exposure, absorbed dose, and effective or equivalent dose. The *absorbed dose* is the amount of energy deposited per unit mass. The *effective* or *equivalent dose* is the amount of radiation per unit mass deposited in living tissues. The amount depends on both the tissue and the type of radiation. For many purposes, the two doses are equivalent, as is the *exposure*, which is the free air dose. With the exception of *activity*, a measure of the amount of radioactive material, the other quantities can also be expressed as rates, usually per hour. The various units are given in Table 6.3. To convert from the SI to the non-SI units of dose, multiply by 100 (e.g., 1 Gy = 100 rad).

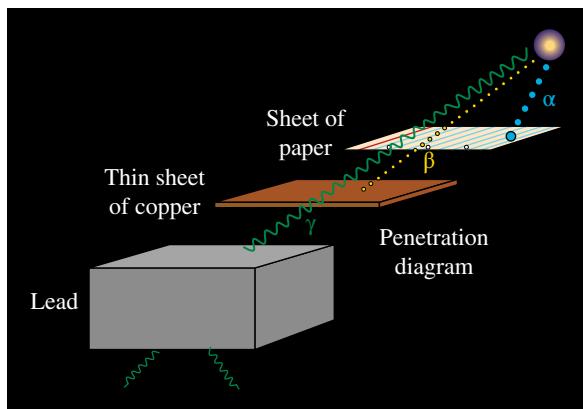
The United Nations Scientific Committee on the Effects of Atomic Radiation evaluates radiation exposure information from each member nation. With this broad purview, they are able to assess the range of exposure to the public and people who

**TABLE 6.2 Neutron Detector Materials**

Detector	Cost	Availability	Comments
$^3\text{He}$	Very high	Limited and declining	
$\text{BF}_3$	Low	High	Good gamma discrimination
Li glass	Very high	Low	
Plastic scintillator	Low	High	Poor neutron discrimination
Li/B-loaded plastic scintillator	Moderate	Moderate	detects both high- and low-energy neutrons
Organic scintillator	Moderate	Limited	Good gamma-neutron discrimination
Liquid scintillator	High	Low	Good gamma-neutron discrimination

**TABLE 6.3 Radiation Units**

Quantity	SI Unit	Non-SI Unit
Activity	Becquerel, Bq	Curie, Ci
Exposure	C/kg	Roentgen, R
Absorbed dose	Gray, Gy	Rad
Equivalent or effective dose	Sievert, Sv	Rem



**FIGURE 6.1** Drawing showing the relative penetration power of alpha ( $\alpha$ ), beta ( $\beta$ ), and gamma rays ( $\gamma$ ). Note that even though alpha and beta particles are stopped very quickly, often X-rays are produced in the process, which are as penetrating as gamma rays. *Source:* The A, B, C's of Nuclear Science. (n.d.). *Experiment #4: Penetrating Power.* Nuclear Science Division of Lawrence Berkeley National Laboratory. Retrieved February 20, 2015, from <http://www.lbl.gov/abc/experiments/Experiment4.html>.

have higher than average exposure through professional work. Through the member nations' efforts, dose monitoring and medical outcomes are cataloged and analyzed. The worldwide average exposure has been estimated to be 2.4 mSv/year (United Nations Scientific Committee on the Effects of Atomic Radiation (UNSCEAR) 2008), which works out to be  $0.27 \mu\text{Sv/h}$  (microSv/h). Most people have exposures from 1 to 13 mSv annually.

The physical effects of radiation depend on both its type and its energy. More energetic radiation is more damaging to living tissues, but the depth to which radiation can penetrate determines how much tissue can be affected (see Fig. 6.1). Alpha radiation has little penetrating power and is stopped by a few inches of air, a piece of paper, or the surface layers of the skin, but causes more damage to the tissues it reaches than do beta and gamma radiations. Alpha emitters can be especially dangerous if ingested or inhaled.<sup>3</sup> A few feet of air, or a thin layer of metal, stops beta radiation. It penetrates through the skin and is moderately damaging and also represents a significant internal medical hazard if taken into the body. The most serious external threat is from isotopes that emit gamma rays. Unlike the electrically charged alpha and beta particles, gamma rays easily penetrate most materials, including all but thick layers of lead or concrete, and can penetrate deep into, and even entirely through, the body. The higher the energy of the gamma ray, the further it can penetrate.

Ionizing radiation can interact with the atoms in your body and strip electrons (ionize) or break chemical bonds. These effects can damage critical structures in cells and cause cells to die or malfunction. Since the body has repair mechanisms, and in general is fairly resistant to radiation damage, the amount of exposure experienced is

<sup>3</sup> Cf. the case of the polonium-210 poisoning of Mr. Alexander Litvinenko.

a useful predictor of health problems. At low levels of exposure (even far exceeding normal levels), we may, or may not, see adverse health outcomes. Very small amounts of radiation, especially if exposure is sporadic, do not appear to increase the likelihood of developing cancer (UNSCEAR 2012) and may even be beneficial (UNSCEAR 2006). As the radiation dose rate, and duration of that dose, increases, biological effects become malign, if not certain to manifest. By the time roughly 1 Sv is received, prompt or deterministic effects begin to occur. It is estimated that approximately 50% of the people who receive 5 Sv will die within 30 days, even assuming adequate hospital care. Without care, death would occur sooner and in higher fractions of highly exposed victims. With current medical capabilities, survival after a 10+ Sv exposure event is not currently considered possible.

To place these exposures in context, recall that the average person receives about 0.27  $\mu\text{Sv}/\text{h}$  normally. Were a person to be exposed to a dose rate of about 5  $\text{Sv}/\text{h}$ , or about 20 million times normal background, for, say, 20 min, he would already have received a life-threatening dose. A pea-sized amount of Cs-137 placed under a train or bus seat would be sufficient to endanger most of the nearby passengers, but prompt detection and remediation can reduce the hazard to an acceptable level.

### 6.3 RADIATION THREAT SCENARIOS

There are several different ways that radioactive materials can be employed to threaten the public. These range from the emplacement of radioisotopes (radiation-emitting device (RED)) to the explosively propelled wide distribution of such material (radiation dispersal device (RDD)) and to the use of nuclear weapons and the resulting neutron activation of the debris (fallout).

An **RED**, also called a “silent source,” is a low-tech, high-consequence attack in which radioactive material is put in a place where the emitted radiation can harm bystanders. Since it takes a significant amount of radiation to poison someone within an hour or so (see the previous text), an RED must contain a significant amount of radiation in order to be effective, though very long exposure times to lower amounts of radiation can also represent a hazard. The resulting high dose rate makes them susceptible to detection—as long as there are nearby detectors.

The **RDD**, also called a “dirty bomb,” uses conventional explosives to widely spread radioactive materials. Numerous analyses of dirty bomb threat scenarios have assessed that the most likely outcomes of such an attack would include a relatively small number of casualties from the detonation itself and moderately to massively disruptive radioactive contamination of the surrounding region (Levi and Kelly 2002; Medalia 2004). Human and economic disruption could be extensive under some circumstances. Some estimates have suggested that the total cost, inclusive of damage, disruption and remediation could exceed \$100 billion (Levi and Kelly 2002).

**Nuclear weapons and improvised nuclear devices (INDs)** both use a warhead of fissile nuclear material (i.e., uranium or plutonium) to create a vast, sudden release of energy. A true nuclear weapon might produce an energy yield equivalent to the detonation of from tens of thousands of tons of TNT (“tens of kilotons” or kT) to

10+ millions of tons of TNT (10 MT). INDs are expected to have yields below several kT. The city-scale destruction of these weapons would require a national-level response (Federation of American Scientists 2013). However, local emergency response teams and first responders would still need to cope with the radiological aftermath of such a scenario, especially in the critical initial hours of such an emergency. Fallout monitoring and the concept of operations (CONOPS) to facilitate personal exposure measurements are discussed in Section 6.5.

Of the three scenarios, REDs are of greatest concern in transportation systems. For a terrorist, a nuclear weapon, whether improvised or not, would be better employed at, or above, street level. Even if transported by well-monitored public transit, plutonium and, especially, uranium are very difficult to detect. RDDs are not a threat particular to transportation systems as they could be detonated anywhere. Depending on the size of the explosive and quantity of radioactive material, a larger, more widely targeted, disruptive effect can be achieved outside the confines of transportation infrastructure. On the other hand, they can be detected during transport prior to delivery, although shielding can hinder discovery.

With REDs, exposure of the radioactive material *is* the attack methodology. Any such attack leaves the material open to detection, provided that radiation detection equipment is present to give prompt warning that an attack is in progress. However, technology is not sufficient to achieve ongoing security. Without appropriate information-gathering procedures, CONOPS, and skills at applying these tools (tradecraft), the technology is merely interesting and cannot, by itself, ensure any level of security.

## 6.4 POLICY AND INTELLIGENCE

There exists a need to properly utilize technological and nontechnical tools to collect information that is accurate, reliable, and timely. The key input to any decisions made about security preparation and actions, whether enforcement or preventative, is sound intelligence about the plans, actions, and motivations of the potential adversary. Without intelligence, it is, indeed, impossible to take any action at all other than to attempt to protect against all threats from all directions and adversaries at all times. Clearly, such a posture is expensive and inefficient. In practical terms, it cannot be achieved.

Since we cannot achieve omniscience, the correct policy is to seek out intelligence about who our adversaries might be, what hostile acts they might plan against us, and when and where they might strike. With the understanding that the boundaries are fuzzy, intelligence can roughly be categorized as deterrent intelligence, defensive intelligence, and offensive intelligence. *Deterrent* intelligence consists of collecting enough information so that an adversary is uncertain of success and must doubt his ability to achieve surprise. *Defensive* intelligence involves learning the adversary's plans in enough detail to deploy one's own forces and resources so as to defeat a specific threat. Finally, *offensive* intelligence permits friendly forces to strike directly at potential adversaries doing harm to their forces and thwarting their plans.

Think of offensive intelligence as special operations crossed with cyber war. Its purpose is active disruption of a terrorist cell's operations and the interdiction of a plot in motion. In the traditional sense, it is not military intelligence at all, but a form of low-level warfare. Offensive intelligence is frequently the executive arm for those organizations that provide information. Making that distinction, we will look only at defensive and deterrent intelligence, as they are more relevant to the role of transportation security organizations. For simplicity, we group them both into a field reasonably called *knowledge intelligence*, or simply KINT.

In the realm of security against radiological attack, one must distinguish between small attacks and very large, crippling ones. Small radiological attacks can go down in scale to the level of a single person or perhaps up to a handful of people. It is fairly likely that attackers with such goals would possess small means and therefore use an unsophisticated means of delivery. For example, an attack could consist of detonating an explosive charge in proximity to a sealed source (e.g., powdered cesium chloride) and allowing the explosive to perform the tasks of opening the shielding and dispersing the contents.

It is unlikely that the usual means of penetrating a terrorist cell is of much value in such an instance because of the small number of participants and the small signatures of a plot in motion. It may be as hard to gain useful intelligence on such a plot, as it was to discover any of the lone gunmen who have killed scores of Americans in the past few years. They had no partners, and much of the isotopes and equipment can similarly be acquired without a sophisticated criminal enterprise.

Deterrent intelligence can be useful in countering radiological terrorism, but it is likely to be expensive. A widespread network of sensors coupled with aggressive efforts to protect radioactive sources from theft or misuse can make it difficult for criminals to engage in a plot to divert and disperse radioactive materials. In contrast to most intelligence efforts that hide in the shadows, most information about deterrent efforts *should* be open. That openness operates to convince potential radioterrorists that there is very little hope that they can execute a strike of more than a very localized effect. As transit and other transportation systems employ detection measures, they ought to consider publicizing those measures.

To be valuable, KINT must have certain properties. Above all, it must be *accurate*. For all the effort that went into the raid that killed Osama bin Laden, the mission would have been a failure if the SEALS had been given the wrong address or the wrong schedule for bin Laden and his associates. This sort of intelligence failure happened in the opening hours of the Iraq War when much effort was put into a direct strike on Saddam Hussein while he slept somewhere else that night.

KINT must also be *timely*. Identifying a threat after it is executed is useless. US intelligence decrypted the message from Tokyo to Japanese diplomats in Washington containing the details of the Pearl Harbor attack together with orders to burn their secret papers and deliver an ultimatum to the State Department in the morning. A flash message alerting US forces in Hawaii was dispatched hours before the attack, but it was misrouted via Western Union and was pigeonholed overnight in Honolulu. A messenger delivered it after the bombs had fallen. We learn from this episode that it is critical that detection systems be able to deliver their information

promptly and to the right people. Detectors must be able to communicate their results automatically and not be dependent upon potentially distracted individuals to pass the message along. Systems must *reliably* ensure the delivery of critical information to key stakeholders. Such information cannot sit, unnoticed, while attackers execute their plan.

In contrast to the intelligence failure cited previously, the US Navy's radio interception analysts at Pearl Harbor detected indications that the Japanese fleet planned a massive invasion of Midway Island along with islands in the Aleutian chain. A bit of radio trickery enabled the US carrier strike force to sortie undetected and to surprise the Japanese with devastating results. The United States would have defeated Japan eventually, but not as soon. The Pacific War hinged on the interception of Japanese communications, providing KINT that was not only accurate and timely but was also detailed enough to be *actionable*. Knowing when, where, and in what strength your enemy will strike is far more useful than simply knowing he would like to do you harm sometime next month, somewhere, and somehow.

Accuracy, reliability, timeliness, and “actionability” are the characteristics that make intelligence worth the costs and risks required to obtain it. From a radiological perspective, it is only through the use of radiation detection technologies that any intelligence may be gathered. Consider, then, these four factors as applied to protecting transportation systems from radiation threats.

*Accuracy and Reliability:* For the information to be useful, it must be trustworthy. The reading itself must be reasonably accurate. The device must be reliable. Its communications pathways must be robust against failure and tampering. In short, there must be no doubt that an alert should be taken seriously. Excessive numbers of false positive alarms rapidly lead to distrust, dismissal, and eventually the removal of the offending device or technology. Excessive failures of information pathways, be they computer network or human messengers, likewise lead to a failure of the system to be reliable and therefore render it unusable.

*Timeliness:* As discussed previously, timeliness of notification requires either dedicated personnel who have no other (primary) duty or a data link to headquarters, wherever it may be. Most security personnel, indeed nearly all first responders, have primary duties that would prevent them from routinely monitoring radiation detection equipment. Portal monitors are a clear exception since they are fixed, high-value, high-cost facilities that command the presence of trained staff. Portable detectors, by contrast, are almost always carried by personnel who have other primary duties; they require that an officer maintain awareness of an auxiliary device that is often perceived as extraneous. To ensure that critical information is delivered in a *timely* fashion, network connectivity that bypasses the possessor of the device is therefore essential for all portable detectors.

*Actionability:* Ultimately, security must be able to *do* something with this information. If an alert is timely and accurate but of too broad a nature, its utility is greatly diminished. As an example, if the sole radiation monitor in a large concourse detects radiation, there is little that can be done immediately. However, if there are several monitoring stations throughout the facility, the approximate location of the source can be quickly inferred or calculated, making subsequent safety and

security operations more focused and therefore more effective and safer for everyone. Again, though, this higher-level analysis needs to be timely and accurate, so automatic systems are indicated.

We now consider these concepts in terms of radiological KINT CONOPS and their impact on acquisition policy.

Each radiation detection technology has strengths and weaknesses. There is no silver bullet. In many cities, the transit infrastructure presents a vast, sprawling, high-value target that has large numbers of customers passing through on a daily basis. Similarly, ports, rail stations, intermodal freight transfer facilities, and other transportation elements are large, vulnerable components of critical infrastructure. Due to the distributed nature of the vulnerabilities presented, it is clear that high-sensitivity portal sensors are incompatible with collecting the KINT needed to protect the whole system and all of its users. Such technologies have a role in high-profile locations but are too costly for pervasive use. Accepting a near-complete lack of radiological KINT elsewhere is unacceptable. So what does the proper selection of technologies and CONOPS look like?

There is a need to balance requirements for coverage, sensitivity, timeliness, and reliability with the realities of innocent alerts (e.g., from the detection of certain medical patients) and cost. Compromises must be made. A good starting point is to use a combination of detector technologies to first achieve comprehensive, if basic, areal coverage and then to supplement with more sensitive devices, likely in the hands of trained personnel. In this way, the system benefits from ubiquitous radiation threat detection and puts powerful tools in the hands of security forces who can quickly provide definitive answers as to the nature, and location, of such a threat. Ensuring the system is tuned to ignore innocent positive detections of the very low level of radiation from a patient treated with nuclear medicine is a key benefit of this approach.

An example of such a layered system might employ four different technologies<sup>4</sup>: (i) broad area coverage provided by opportunistic use of security cameras in combination with GammaPix™ radiation detection software; (ii) randomly roving coverage provided by a fraction of the security forces armed with personal radiation detectors (e.g., CANBERRA UltraRadiac™ or Radiagem™, Thermo-Scientific RadEye™, D-tect Systems mini rad-D™, or RAE Systems GammaRAE II R™); (iii) follow-up expert evaluation provided by specially trained personnel who carry detectors that provide detailed information about the specific isotopes involved in the incident (e.g., CANBERRA InSpector™, Thermo-Scientific RIIDEye™, D-tect Systems rad-ID™, or FLIR identiFINDER™); and (iv) if there are extremely high-profile or high-consequence venues attached to the transportation system, advanced portal monitoring equipment may be required in one or more locations. Other system designs are certainly possible, but the key element that ought to be considered is the creation of a layered set of technologies to satisfy as many requirements, as

<sup>4</sup>Mention of a particular product should not be considered an endorsement of the particular product or company mentioned and is meant to be illustrative rather than prescriptive. Named example products are those on the market at the time of this writing.

comprehensively as can be afforded, in order to collect accurate, reliable, timely, and actionable intelligence.

## 6.5 TECHNOLOGY AND ASSOCIATED CONOPS

Regardless of what sort of KINT is collected and how it is gathered, a robust plan needs to be in place to prevent or overcome radiation emergencies. Whether trying to detect, track, and interdict radiological materials or to assess the extent of a radioactive fallout plume, it is necessary to use radiation detection equipment. With only one exception,<sup>5</sup> these devices need to be procured and prepared prior to any event.<sup>6</sup> Dedicated radiation detection equipment (described previously) has significant lead time for acquisition, training, and deployment.

Once equipment is on hand and personnel are trained, what needs to be done? The answer depends upon the nature of the radiological threat, what detection equipment is available, what protective or survey equipment is available (e.g., is a heavily shielded and thoroughly sealed vehicle available? An unmanned ground vehicle (UGV)?), and who is responding—first responders or experts in the field of radiation emergency management (e.g., a State Police radiation detachment or a National Guard Civil Support Team).

The guiding principle in establishing procedures and CONOPS is to keep as many people as safe as possible while trying to save as many people as possible from an emergency zone. The rule for dealing with radiation exposure is known as “as low as reasonably achievable” (ALARA). Consistent with the principle of ALARA, seek to:

- Minimize time near a source.
- Maximize distance from a source.
- Maximize the amount of shielding between you and the source.
- Ensure that a radioactive material does not enter your body via ears, eyes, mouth, nose, or cuts and by not being immersed in contaminated liquids.

ALARA means always trying to minimize exposure, given the constraints of what needs to get done. It is important to understand that sometimes evacuation from a contaminated zone is necessary and advisable, but other times, it is advantageous for people in an affected region to shelter in place. That decision will be made by experts taking into consideration many factors, including, among others, the source, amount,

<sup>5</sup>GammaPix™ software can be downloaded and run on unmodified Android and iOS smartphones to detect gamma-ray threats. See <http://GammaPix.com> for relevant information.

<sup>6</sup>Portal monitors, typically costing \$100,000 to ~\$1,000,000, are generally used at borders, ports, and high-value venues and require careful emplacement and staffing. Permanent detectors require site preparation for power and any thermal and weather protection. Those sensors that have network connectivity also require access points. Even portable scintillators and G–M detectors need to be purchased and distributed to responding personnel prior to an emergency. All require ongoing maintenance to ensure they are ready for use.

and nature of radiation; the weather; the availability of adequate protective structures; the options and efficacy of evacuation routes; the traffic; and the local geography.

There is no one answer that serves all cases. In addition to the instantaneous blast effects, a nuclear weapon creates an enormous amount of short-lived contamination from the massive neutron pulse. Much of this radioactivity dies down after roughly a week, making sheltering-in-place in a sealed basement a reasonable alternative to venturing out into a contaminated disaster zone, just to be stuck in traffic and wreckage. On the other hand, someone trapped in a bus near a huge Cs-137 gamma-ray source with its 30-year half-life would do well to evacuate, as quickly as possible, since the thin aluminum or steel siding provides almost no shielding. Similarly, the thick stone walls of the older train stations and the deep tunnels of some metro systems may be favorable places to shelter from nuclear weapons or ground-level RDDs, but an RED placed in a subway car would require evacuation of the train. Prompt guidance from experts is critical in a mass casualty disaster that involves a significant amount of radiation. The security response to a radiological threat must be calm and measured, since panic has the potential to cause casualties disproportionately greater than nearly any radiological threat. Several minutes of exposure to all but the very most powerful sources is unlikely to be permanently damaging; panic is much less forgiving. With this caveat in mind, the sections later identify CONOPS for mitigating issues arising from the threat scenarios discussed earlier.

These CONOPS are not a cookbook for emergency response. They are offered as examples for training officers to leverage as they grow the personal and institutional knowledge of radiological emergency consequence management. Training in basic detector and personal protective equipment is essential, but so is detailed scenario training. Consider the difference between practicing the establishment of a 2 mR/h inner cordon that is realistically sized at 500m for a 3000 Ci Cobalt-60 source and the (minimally useful) activity of creating a 2 mR/h cordon that is just 5m in extent around a training-sized source. Of course, we do not suggest practicing with deadly sources. Alternatives such as establishing a cordon at a much lower dose rate, simulated radiation sources,<sup>7</sup> or even just using an arbitrary, but large, hot zone radius are all acceptable for training purposes. In addition to requiring reasonable levels of training fidelity, it is essential that training be carried out often so that the lessons obtained are internalized and retained should they be needed some day.

### 6.5.1 Detecting a Static Source

The detection of a single, nonmoving (static) radiological source requires the right equipment, at the right location, at the right time, preferably before anyone is injured. The trade-off between sensitivity and cost (see Table 6.1) places limits on the type of coverage that will be available. Where sensitivity at any cost is required (e.g., borders, pier side at ports, extremely high-value venues, etc.), portal monitors provide unbeatable sensitivity and the ability to detect even heavily shielded radioactive emitters. Most places aren't borders or ports, however, and most people aren't highly

<sup>7</sup> Simulated radiological training is an optional feature of the GammaPix software suite.

trained with expensive, specialized detectors. Historically, this gap has been filled with good luck and happenstance (Falvey 2011; Luboš 2011). As the technology to use surveillance cameras and smartphones becomes more available, it may be possible for most communities to have a basic level of radiation awareness (Podsada 2013). With pervasive detection capability, it will become much more likely that static sources will be detected and localized quickly. Each organization will need to establish its own rules for handling radiological source discovery, but certain standard operating procedures appear to be prevalent.

### **Step 1: Confirm the Detection**

When radioactive material is detected, a confirming measurement should be made. If high-sensitivity detection equipment is available, this should be used for confirmation, but in any event, the equipment making the original detection can be monitored for additional time to confirm. If the reading is very low, more than one confirmation reading may be necessary. When radiation levels are very low, it takes a very long time before radiation poses a health risk, so plenty of time is available to avoid false positives.

### **Step 2: Request Assistance and Establish Control**

Follow approved procedures to request assistance, often from specially trained personnel (e.g., specially trained transportation security, Transit/Local/State Police units, Civil Support Teams, etc.), and control the area to protect the public and responders. Keep in mind the goal to keep radiation exposure ALARA, and the path to achieve that goal for affected victims may be a prompt evacuation, or it may be for them to shelter in place if a suitably protected site exists.

### **Step 3: Establishing Safe Perimeters**

When the presence of a radiological source has been confirmed, a demarcation must be made between the area people need to avoid and elsewhere. Often, three zones will be established: an inner cordon that is “hot,” an access-controlled zone, and finally the outer cordon beyond which the public may be present in relative safety without interfering with incident management. It has been stated that  $20\text{ }\mu\text{Sv/h}$  ( $2\text{ mR/h}$ ) is as close to a universally agreed-upon stand-off distance as one is likely to find. To determine the location of this demarcation line, measurements should be made in several locations to mark where the inner cordon should be established.

A region of controlled access outside of the inner cordon is generally important, but even more so when there is a radiation threat. This middle area is where decontamination will take place in order to prevent victims from carrying radiation out to the public or into hospitals where others may become contaminated. All of the usual safety and control issues apply. Significant amounts of water and power are likely to be required.

### **Step 4: Locating a Static Source (Different from Detecting It!)**

If a source is not very powerful, trained personnel can carry a survey meter to home in on the area of highest readings in order to identify exactly where a source is located. However, if the source were to be too powerful, it would be preferable to use

a UGV or robot to locate the threat source. The search pattern will make use of the fact that radiation intensity falls off proportionately to the square of the distance. Therefore, as a survey meter approaches a source, the exposure rate climbs quickly. Each time the distance is halved, the exposure rate quadruples. If the  $20\text{ }\mu\text{Sv/h}$  inner cordon is set at 100 m, by the time someone has approached to 10 m from the source, the exposure rate has climbed to  $2\text{ mSv/h}$ . At 0.25 m, the exposure rate is a dangerous  $800\text{ mSv/h}$  blast of radiation! Distance and shielding should be maximized and time near the source should be minimized. Sending in the UGV is the smart thing to do. If the UGV can push the source into a shielding container and not just find it, so much the better! Keep in mind that concrete provides good shielding and is more likely to be available than lead. For gamma rays from Co-60, each 10 cm thick layer of concrete, or 1 cm thickness of lead, will reduce the dose rate by a factor of 2.

### 6.5.2 Tracking a Moving Source

Tracking a moving source is a hard problem. The best option for dealing with a moving source is to get it to stop. In a transportation environment, stopping the vehicles may be the best alternative, though on surface roads, control over stoplights may be almost as good. Stopping the vehicle with the source allows security to catch up and get ahead of the movement. Simply slowing it down may achieve enough. There are three approaches that a transportation security system can take to track a moving radiation source:

1. Rely on luck: If the source moves past successive sensors, a time-tagged track begins to form. This may be enough information to determine that a source is on a particular train or bus. Or luck may not provide the needed data. In this case, if the alarms are centralized, you may see potential radiation events appearing and disappearing in the system. Personnel monitoring the system must be trained and aware of the possibility of moving threats to deduce that this is the situation.
2. Rely on even more luck: A radiation detector-carrying security officer may be riding the vehicle that has the source. In this lucky case, the officer will have a real-time indicator that there is a nearby source and be able to take appropriate action. The radiation detector will need to be functional, have good batteries, and be turned on, and the officer will need to have had the required training.
3. Be prepared: The use of inexpensive, networked sensors enables pervasive radiation awareness across the transportation facility or transit system and across the city. If each bus and train car has a sensor; if each metro and bus station has many sensors; if ports, airports, and rail stations are well instrumented; if each of these sensors is networked together back to a central monitoring station; and if all of these are true, tracking a moving radiation source can be done in real time. When the sensors are on board, then for those devices, the source is no longer moving. Once detection has taken place, the bus or train can be slowed down enough for security to deal with the incident. People will be spared hours, days, or weeks of dangerous radiation threats traveling the roads and rails.

A variant on this problem occurs when there are multiple moving sources, such as if REDs were to be placed on multiple vehicles. In this case, it may be more difficult to discern the location of the individual sources unless there are detectors on the vehicles themselves.

Once a moving source has been detected, the motion can be brought to a halt in a suitable place and the SOP steps discussed previously can then be implemented.

### 6.5.3 Discovering Multiple Sources

Some threat scenarios suggest that multiple sources of radiation could be placed in a given area, for example, a metro station, in order to increase an attack's impact. In such a case, initial readings might show ambiguous results during the localization phase since readings might go up when moving both forward and backward from a particular location.

Imagine a situation where three sources are placed along a train platform. When standing between two sources, the reading on a detector will increase when walking toward either source. If not prepared to consider the possibility of more than one source, the officer might suspect faulty equipment. Furthermore, if the officer continued past the peak, when right next to a source, the reading would first decrease and then might increase again as the next source was approached.

The solution is to mark the area near each peak reading. After a quick survey, it should be possible to verify and localize each source. In an open area, the situation might be more complicated as movement in two or even three dimensions (forward and backward, left and right, up and down) is possible. In some venues, there may be radiation coming from a lower level of a bus station or a higher floor in a parking garage. Or, alternatively, shielding provided by the building's structure may hide one or more sources from some perspectives. The procedure is the same but requires a systematic survey, noting where peak emissions are located. A contour plot displaying the readings may be very useful. Given the  $20\mu\text{Sv/h}$  stand-off distance, it is possible that multiple sources will combine their fields to create a merged, larger exclusion zone. In such a case, it is likely that a UGV would be needed to safely localize, and render safe, successive sources.

In an environment where many sensors have already been deployed, for example, a station-spanning set of security cameras connected to video analytics, a real-time map of radiation levels at the sensor locations may already exist or can be constructed. In such a case, it is likely that the presence of multiple sources will be immediately apparent, with the map showing which cameras report the highest readings. Localization efforts would then focus on each "island" of highest radioactivity.

### 6.5.4 Assessing Areal Contamination

Similar to the previous case, areal contamination involves radioactive material spread out across some region, as may be the result of an RDD or IND attack. Unlike the previous case, the source of radiation is not a set of discrete pieces that

can just be picked up and put in a lead container. The key to differentiating between fallout and multiple sources is to note the distribution of readings. Areal contamination will show a much smoother distribution with fewer peaks and troughs in the distribution map. Multiple discrete sources, as discussed previously, will lead to sharp peaks of measured radiation near the sources, separated by lower readings far from them.

Decontamination of a region is an entirely separate discipline and is not covered in this text. What is important from a transportation security perspective is that dispersed radioactive material:

- Can spread with wind and water action or by being carried by vehicular, human, or animal traffic
- Can be inhaled or ingested
- Can contaminate open water and become an immersion risk

For this case, the following SOP steps are appropriate.

### **Step 1: Assessment**

Depending on the cause of the problem, it may not be immediately apparent that there is a radiation problem. First responder assessment should routinely include rapid measurement of the radiation environment. Depending on the amount of radiation, and its dispersal, initial readings may not reveal radiation. Ongoing monitoring will eventually detect if there are hot spots, and of course, if the contamination is severe, early readings will detect it. If the affected area is not too large, as with an RDD in a confined space, establishing the  $20\mu\text{Sv}/\text{h}$  inner cordon will facilitate later actions such as setting up decontamination areas and an on-scene command post, if relevant. The other benefit of prompt assessment is knowledge of the extent of area that is contaminated. Wind, blast, and flames can carry contamination long distances. A rapidly moving railcar could also spread material. The takeaway is to learn how to use the equipment you have and use it early and often; keep the batteries charged. If you don't have special equipment, use your smartphone's inherent ability to detect radiation (Medalia 2004).

### **Step 2: Stabilization**

It is important to quickly assess if there is radioactive fallout in order to identify if a protective gear is required for operations within the hot zone. It is possible that fully enclosed suits with compressed air tanks may be required. Early knowledge can save lives.

### **Step 3: Disposition of Victims**

As discussed previously, the science of assessing when to evacuate vice shelter in place (Centers for Disease Control and Prevention 2013) is complicated (Brandt and Yoshimura 2011). Experts can be expected to provide guidance based on the myriad parameters that go into their determination, many of which are particular to the affected region.

**Step 4: Decontamination**

Since hospitals are not equipped to perform mass decontamination, and travel to medical facilities by contaminated individuals would in turn contaminate ambulances, on-scene decontamination will be important. Special units, such as the National Guard Civil Support Teams in the United States, exist and would be involved in these activities. Contamination from fallout is possible even on those who are not injured. Dedicated, sensitive radiation measurement equipment can be used to assess if someone is carrying contamination.

**6.5.5 Finding the Limits of a Contaminated Region  
(e.g., a Fallout Plume from an RDD or IND)**

This scenario, as with the previous, is most likely to emerge from the detonation of an RDD or a nuclear weapon of some sort. Other scenarios exist but are essentially the same in terms of assessment, stabilization of the scene, disposition of victims, and decontamination.

Extending the analysis of contamination from the previous case, nuclear weapon detonations or the plume from a large RDD may produce a vast downwind zone of radioactive fallout. While such a scenario is obviously beyond what even the largest transportation security organization could cope with, each piece of data can help to define the extent of the disaster zone and keep the public and security personnel safe from needless exposure.

If networks have survived and are operational, distributed infrastructure sensors can provide a rough outline of go/no-go zones. Officer-carried sensors can likewise fill out that data. National-level resources will ultimately be needed for rescue and recovery operations, but as with previous scenarios, early information can save lives and inform decisions as to where resources are most needed. Keep the batteries charged!

**6.6 SUMMARY AND CONCLUSIONS**

Many security experts believe a radiological or nuclear attack is inevitable. The operational consequences for the impacted location, let alone the personal cost, force us to face this grim probability with resolve and vigorous mitigation efforts. This chapter discusses consequence management in the aftermath of a nuclear or radiological attacks and the nature of the resulting hazards. The three legs upon which these responses rest are the appropriate use of detection technology, the suitable intelligence collection techniques, and the distillation of tactics, techniques, and procedures into effective CONOPS.

Since radiation detection can only be done with appropriate equipment, we recommend a variety of such equipment be employed in a layered approach. These should be chosen to complement each other and provide both wide and precision detection capability. The intelligence provided by this equipment must be accurate, timely, and actionable. Integration with other intelligence and decision-making tools

is strongly recommended. It is through training, administered early and often, that security personnel can fuse knowledge of equipment and procedural know-how into an effective prevention and mitigation strategy.

## REFERENCES

- Brandt, L. D., & Yoshimura, A. S. (2011). Analysis of Sheltering and Evacuation Strategies for a Chicago Nuclear Detonation Scenario (SAND2011-6720). Retrieved from <http://prod.sandia.gov/techlib/access-control.cgi/2011/116720.pdf> (accessed February 20, 2015).
- Centers for Disease Control and Prevention (2013, August 22). CDC Radiation Emergencies | Sheltering in Place During a Radiation Emergency. Retrieved March 2014, from <http://emergency.cdc.gov/radiation/shelter.asp> (accessed February 20, 2015).
- Falvey, C. (2011). Radio Prague—Passerby Stumbles Upon Radioactive Playground Thanks to Wristwatch. Retrieved from <http://www.radio.cz/en/section/curraffrs/passerby-stumbles-upon-radioactive-playground-thanks-to-wristwatch> (accessed February 20, 2015).
- Federation of American Scientists. (2013). Nuclear Weapon Effects Calculator. Retrieved from [http://www.fas.org/programs/ssp/nukes/nuclear\\_weapon\\_effects/nuclearwpneffctcalc.html](http://www.fas.org/programs/ssp/nukes/nuclear_weapon_effects/nuclearwpneffctcalc.html) (accessed February 20, 2015).
- Levi, M. A., & Kelly, H. C. (2002, November). Weapon of Mass Disruption. *Scientific American*, p. 76.
- Luboš, M. (2011). The Reference Frame: Why a Small Cylinder Buried in Prague Radiates 500  $\mu$ Sv/h? Retrieved from <http://motls.blogspot.ca/2011/09/do-they-have-500-sv-in-prague-and-why.html> (accessed February 20, 2015).
- Medalia, J. E. (2004). *Terrorist “Dirty Bombs”: A Brief Primer (RS21428)*. Washington, DC: Congressional Research Service, Library of Congress.
- Podsada, J. (2013, March 19). Dirty Bombs: A Smart Phone Application That Measures Radioactivity Could Detect Dirty Bombs—Hartford Courant. Retrieved from [http://articles.courant.com/2012-03-19/business/hc-smart-phone-geiger-counter-20120319\\_1\\_gamma-rays-radiation-apple-app](http://articles.courant.com/2012-03-19/business/hc-smart-phone-geiger-counter-20120319_1_gamma-rays-radiation-apple-app) (accessed February 20, 2015).
- Rubenstein, E. P., & Drukier, G. (2009). Detection of Radioactivity in Transit Stations—Phase 2. Final report submitted to Transportation Research Board of the National Academies. Retrieved from [http://onlinepubs.trb.org/onlinepubs/idea/finalreports/transit/transit54\\_final\\_report.pdf](http://onlinepubs.trb.org/onlinepubs/idea/finalreports/transit/transit54_final_report.pdf) (accessed February 20, 2015).
- United Nations Scientific Committee on the Effects of Atomic Radiation. (2006). Effects of Ionizing Radiation. Retrieved from [http://www.unscear.org/docs/reports/2006/07-82087\\_Report\\_2006\\_Web.pdf](http://www.unscear.org/docs/reports/2006/07-82087_Report_2006_Web.pdf) (accessed February 20, 2015).
- United Nations Scientific Committee on the Effects of Atomic Radiation. (2008). Sources and Effects of Ionizing Radiation. Retrieved from [http://www.unscear.org/docs/reports/2008/09-86753\\_Report\\_2008\\_Annex\\_B.pdf](http://www.unscear.org/docs/reports/2008/09-86753_Report_2008_Annex_B.pdf) (accessed February 20, 2015).
- United Nations Scientific Committee on the Effects of Atomic Radiation. (2012). Biological Mechanisms of Radiation Actions at Low Doses. Retrieved from [http://www.unscear.org/docs/reports/Biological\\_mechanisms\\_WP\\_12-57831.pdf](http://www.unscear.org/docs/reports/Biological_mechanisms_WP_12-57831.pdf) (accessed February 20, 2015).

---

# 7

---

## PROTECTING TRANSPORTATION INFRASTRUCTURE AGAINST RADIOLOGICAL THREAT

ILAN YAAR, ITZHAK HALEVY, ZVI BERENSTEIN, AND AVI SHARON

*The Nuclear Research Center Negev (NRCN), Israel Atomic Energy Commission (IAEC), Negev, Tel Aviv, Israel*

### 7.1 INTRODUCTION

Public transportation systems such as ships, airplanes, trains, ferries, underground trains, and buses are essential elements in a developed country's economy. As learned after the 9/11 attack (Lubenuau and Storm 2002; Makinen 2002), a terror attack on this complex system may cause thousands of casualties and significant economic damage. The attack can be a conventional one, like the train bombing in Spain (Reinares 2010) or the bus bombing in London (Murphy 2006), or a nonconventional one, like the sarin attack on the underground train in Tokyo, Japan (Tu 1999). A radiological attack on the transportation system is also feasible (Office of Intelligence and Analysis 2006). This type of attack must be taken into consideration due to the vulnerability of this infrastructure to such an attack and the severe economic outcome of it (Acton et al. 2007; Zimmerman and Loeb 2004).

The radioactive material that might be used by terrorists in order to attack any type of transportation infrastructure was recently identified and categorized in two of the International Atomic Energy Agency (IAEA) Nuclear Security Series publication (IAEA 2004a, 2005). The most common and therefore accessible radionuclides are the gamma emitters  $^{60}\text{Co}$ ,  $^{137}\text{Cs}$ , and  $^{192}\text{Ir}$ ; the beta emitter  $^{90}\text{Sr}$ ; and the alpha emitters

**TABLE 7.1 The Most Common Radioactive Materials Used in the World, their Most Common Applications, and their Nuclear Properties**

Application	Radionuclide	Half-life (Y)	Activity
Radiotherapy	Co-60	5.30E+00	50–1000 TBq
	Cs-137	3.00E+01	500 TBq
Industrial radiography	Ir-192	2.00E-01	0.1–5 TBq
	Co-60	5.30E+00	0.1–5 TBq
Sterilization	Co-60	5.30E+00	0.1–400 PBq
	Cs-137	3.00E+01	0.1–400 PBq
	Sr-90 (Y-90)	2.90E+01	50–1500 MBq
Well monitoring	Cs-137	3.00E+01	1–100 GBq
	Am-241	4.32E+02	1–800 GBq
Level and thickness gauges	Cs-137	3.00E+01	10 GBq–1 TBq
	Co-60	5.30E+00	1–10 GBq
Density detector	Am-241	4.32E+02	0.1–2 GBq
	Cs-137	3.00E+01	Up to 400 MBq
	Ra-226	1.60E+03	~1500 MBq

*Source:* International Atomic Energy Agency and L.A. Bolshov, Objective and Subjective Impediments to the Broad and Successful Application of Ionizing Radiation Sources, in Safety and Security of Radioactive Sources: Towards a Global System for the Continuous Control of Sources Through Their Life Cycle, Proceedings of an International Conference held in Bordeaux, June 27–July 1, 2005, International Atomic Energy Agency, Vienna (2006), p. 283. Reproduced with permission from IAEA.

$^{241}\text{Pu}$ ,  $^{238}\text{Pu}$ , and  $^{241}\text{Am}$ . The properties of these radionuclides, reproduced from IAEA and Bolshov (2006) with permission from the IAEA, are listed in Table 7.1.

The radioactive sources made from these radionuclides are divided into five categories, according to the risk they pose in the event of a radioactive material dispersion. The risk level is mainly determined by a typical source total activity,  $A$  (measured in curies or Bq), normalized by the source-specific activity,  $D$  (measured in curies or Bq per gram), after consideration of other factors, such as the physical and chemical forms, the type of shielding or containment employed, and the circumstances of use and accident case histories (Zimmerman and Loeb 2004). The IAEA categorization of these sources, reproduced from IAEA (2004a) with permission from the IAEA, is listed in Table 7.2. Category 1 sources are the most dangerous ones; these sources must be kept under secure conditions due to the risk they pose in a case of an accident or a deliberate use of them by terrorists.

A radiological event can be any of two principle scenarios. In the first scenario, a radiological dispersal device (RDD) or “dirty” bomb is used (Schmid 2000). This device consists of a radiation source that is detonated using conventional or improvised explosives (Sohier and Hardeman 2006). Most of the casualties in this event will be from the explosion blast wave. However, some people might become contaminated with different levels of radiation (Slater et al. 2003), some might need to go through some type of medical screening process, and the costs of the total actions might be significant (Musolino and Harper 2006).

The second scenario involves a silent dispersion of radioactive material in a public site. In this event, there are no immediate known casualties, and the fact that people

**TABLE 7.2 Activities Corresponding to Selected Radiation Source D Value Categories**

Radionuclide	Category 1 $1000 \times D$ (TBq)	Category 2 $10 \times D$ (TBq)	Category 3 $D$ (TBq)
Am-241	6.00E+01	6.00E-01	6.00E-02
Am-241/Be	6.00E+01	6.00E-01	6.00E-02
Cf-252	2.00E+01	2.00E-01	2.00E-02
Cm-244	5.00E+01	5.00E-01	5.00E-02
Co-60	3.00E+01	3.00E-01	3.00E-02
Cs-137	1.00E+02	1.00E+00	1.00E-01
Gd-153	1.00E+03	1.00E+01	1.00E+00
Ir-192	8.00E+01	8.00E-01	8.00E-02
Pm-147	4.00E+04	4.00E+02	4.00E+01
Pu-238	6.00E+01	6.00E-01	6.00E-02
Pu-239/Be	6.00E+01	6.00E-01	6.00E-02
Ra-226	4.00E+01	4.00E-01	4.00E-02
Se-75	2.00E+02	2.00E+00	2.00E-01
Sr-90 (Y-90)	1.00E+03	1.00E+01	1.00E+00
Tm-170	2.00E+04	2.00E+02	2.00E+01
Yb-169	3.00E+02	3.00E+00	3.00E-01
Au-198 <sup>a</sup>	2.00E+02	2.00E+00	2.00E-01
Cd-109 <sup>a</sup>	2.00E+04	2.00E+02	2.00E+01
Co-57 <sup>a</sup>	7.00E+02	7.00E+00	7.00E-01
Fe-55 <sup>a</sup>	8.00E+05	8.00E+03	8.00E+02
Ge-68 <sup>a</sup>	7.00E+02	7.00E+00	7.00E-01
Ni-63 <sup>a</sup>	6.00E+04	6.00E+02	6.00E+01
Pd-103 <sup>a</sup>	9.00E+04	9.00E+02	9.00E+01
Po-210 <sup>a</sup>	6.00E+01	6.00E-01	6.00E-02
Ru-106 (Rh-106) <sup>a</sup>	3.00E+02	3.00E+00	3.00E-01
Tl-204 <sup>a</sup>	2.00E+04	2.00E+02	2.00E+01

*Source:* Data taken from the International Atomic Energy Agency, Categorization of Radioactive Sources, IAEA Safety Standards for Protecting People and the Environment, Safety Guide No. RS-G-1.9, International Atomic Energy Agency, Vienna (2005), p. 45. Reproduced with permission from IAEA.

<sup>a</sup>These radionuclides are very unlikely to be used in individual radioactive source with activity level that would place them within category 1, 2, or 3.

were exposed to radioactive material will be discovered only in the uncommon event when symptoms of radiation sickness will be identified due to exposure to high radiation dose (Acton et al. 2007) or if the radioactive material is discovered by a first responder equipped with a radiation detector or a dosimeter.

The main impact of such a radiological attack is the contamination of a large area (Reshetin and Regens 2005). The size of the contaminated area depends on the type and activity of the radioactive material, on the type and geometry of the dispersion device, on the micrometeorology conditions, and on the cross contamination caused by the movement of people inside the contaminated area (Harper et al. 2007).

A good example for the consequences of a typical radiation contamination and exposure due to either one of the two events can be found in the 1987 Goiania

accident (IAEA 1988). In this event, a shielded, strongly radioactive  $^{137}\text{Cs}$  source (50.9 TBq at the time of the incidence) was accidentally opened, and the radioactive material was dispersed in one of the city's neighborhoods. Consequently, many people were subjected to large doses of radiation, due to both external and internal exposures. Thousands of people went through contamination screening process, hundreds of people were found to be contaminated, 28 of them suffered radiation burns, and 4 of the casualties that were exposed to high radiation levels died.

Two experimental programs, "Green Field" (GF) (Sharon et al. 2010, 2012a) and "Red House" (RH) (Sharon et al. 2011), were recently conducted in Israel in order to increase the preparedness for an RDD event. The GF program aimed at evaluating the consequences of an outdoor and an indoor explosion of an RDD device, while the RH program aimed at evaluating the outcome of a silent dispersion of a radioactive material inside a building.

Based on the results of these two experimental programs, the consequences of a possible RDD attack or a silent indoor dispersion of a radioactive material will be given, and the necessary preventative steps that can be taken in order to secure transportation infrastructure systems against these threats will be specified.

## 7.2 EXPERIMENTAL SETUP AND RESULTS

### 7.2.1 Simulation of an Outdoor RDD Attack

An outdoor explosion of an RDD can be used by terrorists in the attempt to contaminate critical transportation infrastructure such as harbor docks, train stations, bus stations, and airports with radioactive materials. In the last part of the GF program, a set of experiments using the short-lived radioisotope  $^{99\text{m}}\text{Tc}$  were conducted in order to study the consequences of such an event (Sharon et al. 2012b).  $^{99\text{m}}\text{Tc}$  is used in tens of millions of medical diagnostic procedures annually, making it the most commonly used medical radioisotope in the world (Eckelman 2009).  $^{99\text{m}}\text{Tc}$  was used in these experiments because it is easily accessible for a reasonable cost, it has a short half-time period (6.02 h) allowing enough time for data collection and short enough to permit access to the experiment field after several days, and it is also easily detected by its 140.5 keV gamma line using simple gamma detectors.

The main purpose of this phase, conducted between October 2010 and November 2012 at a test field located in the south part of Israel, was to verify the source model that had been developed in the first phase of the program (Sharon et al. 2012a) and to try to evaluate, according to the results, what will be the contamination levels caused by such an event if long-lived radioisotopes, like the ones listed in Table 7.1, are involved.

Overall, 14 tests were conducted using 5–7 Ci of  $^{99\text{m}}\text{Tc}$  bottled in a  $30\text{ cm}^3$  saline water and coupled to 0.25–2.5 kg of TNT, in each test. The surfaces below the charge were packed dirt–sandy soil used to enhance dirt entrainment into the fireball, a clean steel surface used to avoid ambient dirt entrainment into the fireball, asphalt, or concrete that simulates urban surfaces. The amount of dirt in the initial fireball

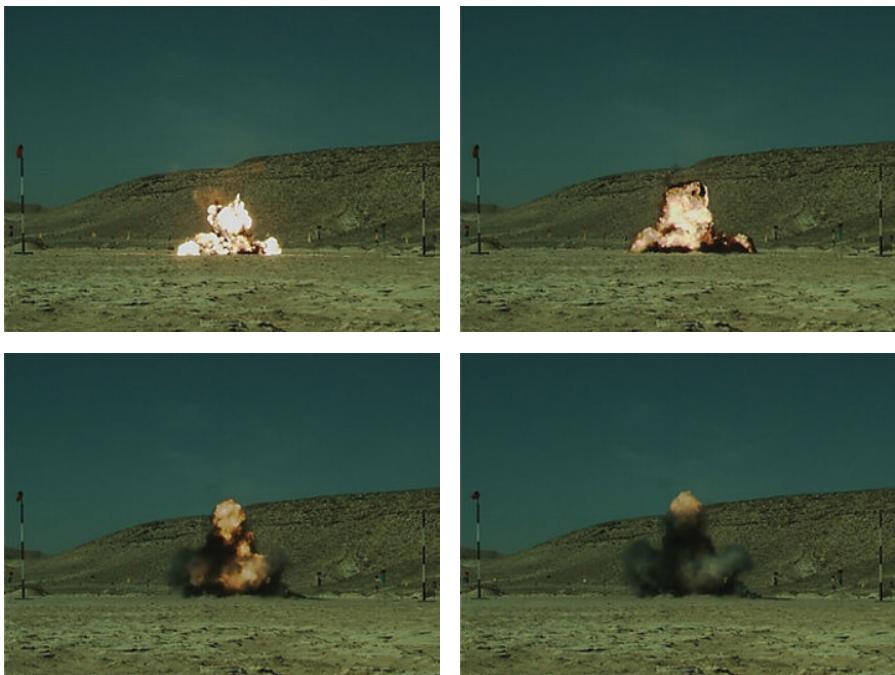
influenced the final particle size distribution and hence the pattern of the surface deposition and the aerial concentration of activity following such an event. All of the experiments' results were recorded by three video cameras (taken from three different angles) and by a high-speed camera, and some of them were also recorded by a thermal infrared (IR) camera.

On-site gamma measurements were taken by several gamma detectors—a small personal detecting system (<https://www.mirion.com/products/radiation-detection-and-protection-instruments/advanced-detection-and-isotope-identification/spectroscopic-personal-radiation-detector-sprd/>) based on a 1" by 1" cesium iodide (CsI) crystal, a laboratory medium resolution detector (<http://www.ortec-online.com/download/Lanthanum-Bromide-Scintillation-Detectors.pdf>) based on a 1.5" by 1.5" lanthanum bromide ( $\text{LaBr}_3$ ) crystal, and a spectral advanced radiological computer system (SPARCS) ([http://nnsa.energy.gov/sites/default/files/nnsa/newsletters/10/NNSA\\_NEWS\\_April\\_2009.pdf](http://nnsa.energy.gov/sites/default/files/nnsa/newsletters/10/NNSA_NEWS_April_2009.pdf)) based on several sodium iodide crystals. A high gamma resolution pure germanium (HPGe) detector (<http://www.ortec-online.com/download/best-choice-high-purity-germanium-hpge-detector.pdf>) was also used at the laboratory in order to count the radioactivity collected via Petri dishes that were placed around the detonation point.

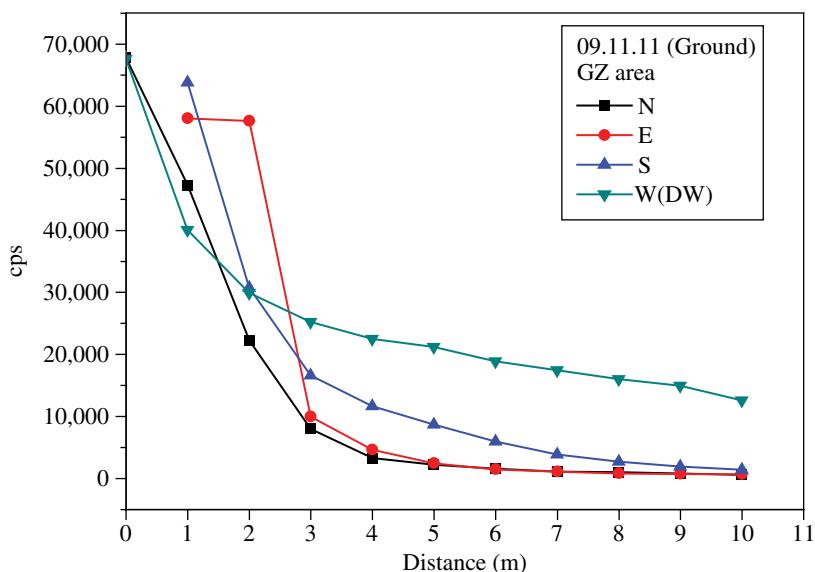
Radiation measurements were taken with both shielded and unshielded  $\text{LnBr}_3$  detectors for local and nonlocal estimation of the radiation field, respectively. The importance of taking both shielded and unshielded measurements is vital for the estimation of the first responder's doses (which includes the influence of the hot spot close to the detonation point) as well as the estimation of the local ground contamination levels.

Some of the results obtained in these experiments are shown in Figures 7.1, 7.2, 7.3, and 7.4. High-speed camera snapshots of the fireball created in the explosion of 2.5 kg of TNT detonated at ground level are depicted in Figure 7.1. The  $\text{LaBr}_3$  detector readings (counts per second) measured several meters from the detonation point is depicted in Figure 7.2. The  $\text{LaBr}_3$  readings for the 0.25 kg and for the 2.5 kg of TNT charges detonated at ground level taken up to 200 m downwind and upwind from the detonation point with and without shielding are depicted in Figure 7.3. The results are plotted in counts per second (cps), corrected for the source radioactive decay. The activity on the ground for one of the 2.5 kg tests, measured with the SPARCS, is depicted in Figure 7.4 in units of  $\mu\text{Ci}/\text{m}^2$ .

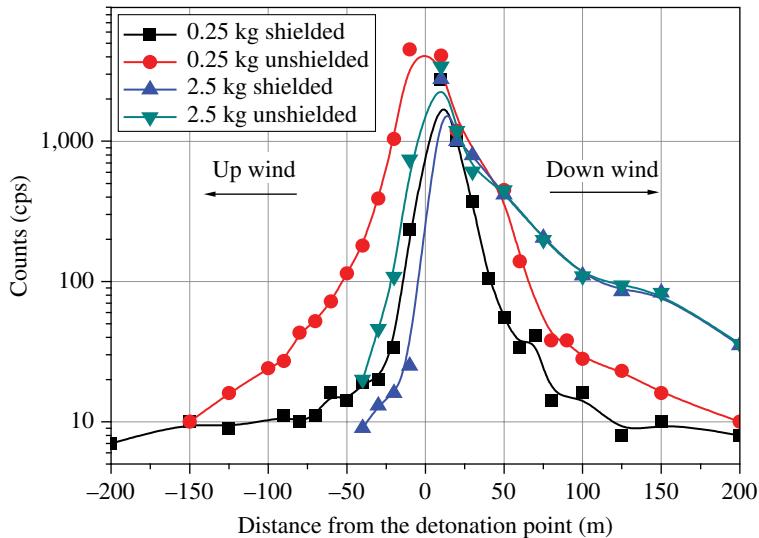
The main findings concluded from these experiments, which can be relevant to a real RDD event inside a critical transportation system, are that about 20% of the total activity is found on the ground close to the detonation point and less than 1% of the original activity is observed on the ground outside of this area. It should be mentioned that this is true only for the cases where most of the particles created were fine aerosols due to the charge geometry and radioactive material type that enhanced the creation of such particles. In cases where most of the particles will be in the ballistic size range ( $>100 \mu\text{m}$  aerodynamic diameter), a reasonable assumption in the case of an RDD made of a metallic  $^{60}\text{Co}$  or  $^{192}\text{Ir}$  source, it is reasonable to assume that most of the particles will settle on the ground within the range of few hundred meters around the point of release due to aerodynamic drag and gravitational settling.



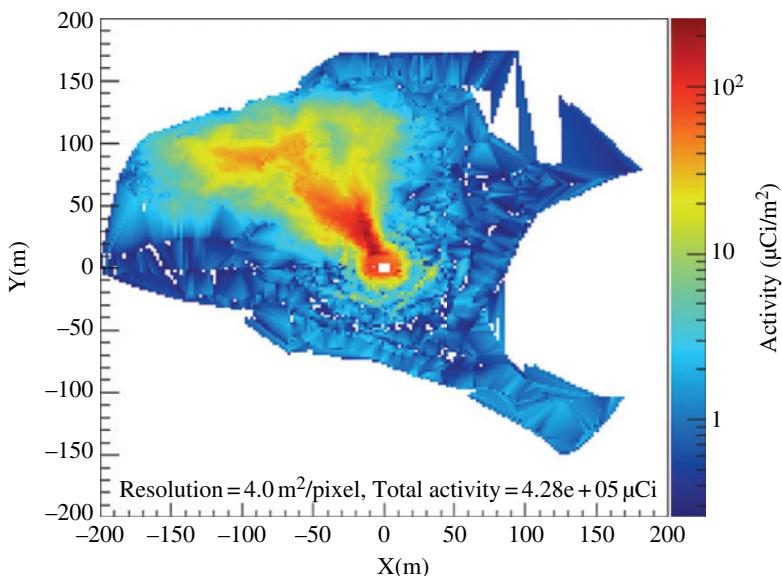
**FIGURE 7.1** Fireball–ground interaction zone snapshots taken by the high-speed camera.



**FIGURE 7.2** Activity distribution inside the GZ area, given in counts per second (cps) and corrected to the radioactive decay.



**FIGURE 7.3** Downwind measurements of the ground contamination after a 0.25 and 2.5 kg TNT charges detonated at ground level. The measurements, taken using a shielded and a non-shielded LaBr<sub>3</sub> detector, are given in units of counts per second (cps), corrected for source radioactive decay.



**FIGURE 7.4** The activity on the ground after a 2.5 kg test, measured with the SPARCS. The results are given in units of  $\mu\text{Ci}/\text{m}^2$ .

### 7.2.2 Simulation of an Indoor RDD Attack

In this section, the results of a set of tests that were conducted in order to measure the consequences of an indoor RDD event are given (Sharon et al. 2010). This scenario is relevant to a terrorist attempt to contaminate critical transportation system buildings, such as train stations, bus stations, and airport terminals, with a radioactive material.

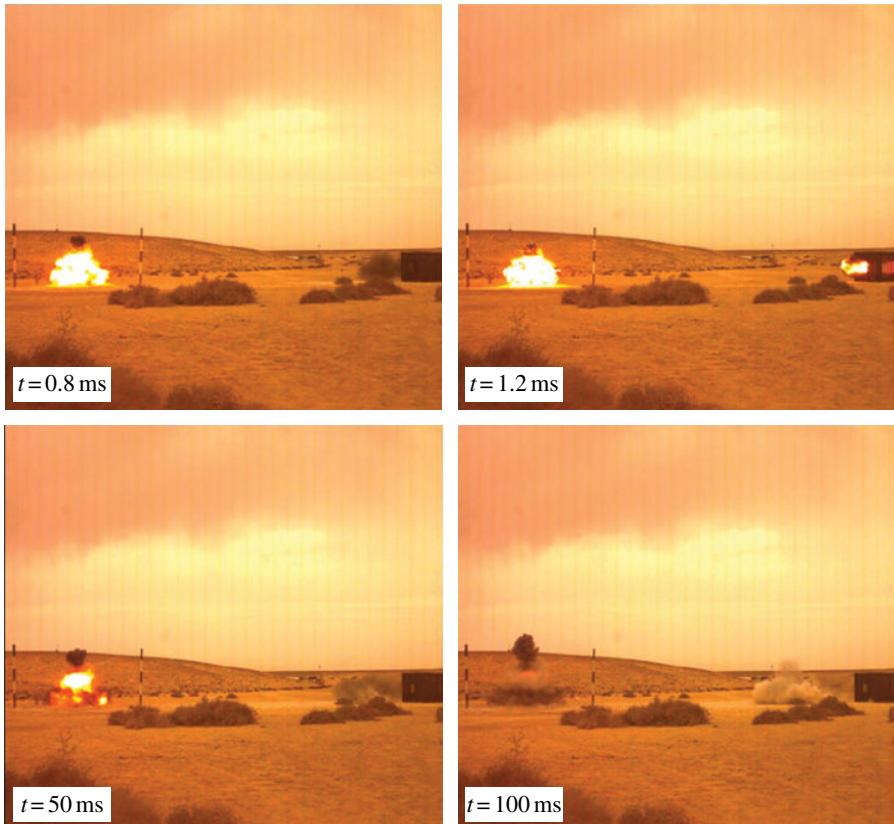
When an RDD is detonated inside a building with openings, part of the radioactive material will contaminate the building, and the rest will be emitted out from doors and windows. In all of the experiments conducted in this part of the program, two identical charges were simultaneously detonated. One charge was placed outdoor and the second one was hanged at the center of a small steel chamber, 3 by 3 by 2 m<sup>3</sup>, with two 1 by 1 m<sup>2</sup> openings in the center of adjacent walls. Test results were recorded by three video cameras and by a high-speed camera, and some of them were also recorded by a thermal IR camera. In addition to comparing between the heights of the clouds created inside and outside of the steel chamber, the amount and the size of the particles that were emitted from the openings after the blast and the distribution of the material inside the chamber were also measured.

Some of the high-speed camera snapshots of simultaneous 1 kg TNT indoor and outdoor explosions are depicted in Figure 7.5. The evaluation of both fireballs as a function of time can be seen and compared in this picture. Some of the video camera pictures taken during the same test are depicted in Figure 7.6. The evaluation of the cloud created for both explosions as a function of time can be seen and compared in these pictures. The cloud created by the indoor explosion is lower than the one created by the outdoor explosion. This finding can be attributed to the fact that part of the explosion energy is absorbed in the structure walls.

In six of the indoor shots, nonradioactive CsCl and SrTiO<sub>3</sub> powders, simulating radioactive sources, were used. After each of these shots, samples were taken from the walls, the ceiling, the floor, and the samplers that were hanged outside of each window. These samples were analyzed using an inductively coupled plasma mass spectrometry (ICP-MS) laser ablation technique, and the average material (CsCl or SrTiO<sub>3</sub>) concentration on these areas was calculated. The results show that within this amount of explosive and chamber size, the material was dispersed homogeneously over the walls and windows area. Therefore, the ratio between the fraction of radioactive material that will be dispersed outside and inside the building in an indoor RDD event will be proportional to the ratio between the total openings' area (doors, windows, etc.) and the total area of the building (including walls, floor, and ceiling).

### 7.2.3 Simulation of a Silent Indoor Dispersion of Radioactive Material

A set of experiments, which included silent dispersion of liquid <sup>99m</sup>Tc, were conducted as a part of the RH experimental program (Sharon et al. 2011). This part of the program was conducted in order to improve the preparedness and response to terrorism scenarios such as silent dispersion of radioactive material inside shopping malls, government offices, or critical transportation system facilities. The tests were



**FIGURE 7.5** High-speed camera shots of the simultaneously indoor and outdoor explosions. The time after detonation in which every picture was taken is written inside every frame.

conducted (on July 2010) in the assigned Chemical, Biological, Radiological and Nuclear (CBRN) Israel Defense Force (IDF) home front command facility located near the town of Ramla.

The risk of individual exposure to radioactive materials inside buildings depends on many parameters, which may include the type of material, the particles' size distribution, the buildings inside geometry, and the airflow pattern inside the building, which may be influenced by the air ventilation system and by people motion.

The main purpose of this part of the program was to estimate the distribution of activity on the floor and in the air inside the building in order to revise the preparedness and response to silent terror activity, including the proper design of cost-effective detection systems for such events inside buildings.

The CBRN training building is designed as a small-size two-floor shopping mall. The main floor (ground floor) is about 24 by 24 m<sup>2</sup> size and includes an empty central part (18 by 18 m<sup>2</sup>) surrounded by shops and offices. The upper floor is gallery-like surrounded by shops and offices from all sides, as shown in Figure 7.7.



**FIGURE 7.6** Video camera shots of the simultaneously indoor and outdoor explosions. The time after detonation in which every picture was taken is written inside every frame.

The building air ventilation system includes five separate units. The first four units are used in order to cool the open space (each one is for about half size of a floor), and the fifth unit is used in order to supply air to the shops and offices area. The system supplies the cool and warm air through closed ducts. The air exchange rate inside the building is in the range of 8–12 changes per hour. The system enables temperature control in each one of the shops and offices. In order to avoid the influence of too many parameters, the air-conditioning system was kept steady during the whole period of the experiment. The temperature was tuned to be in the range of 20–23°C, and the relative humidity was about 40–50%.

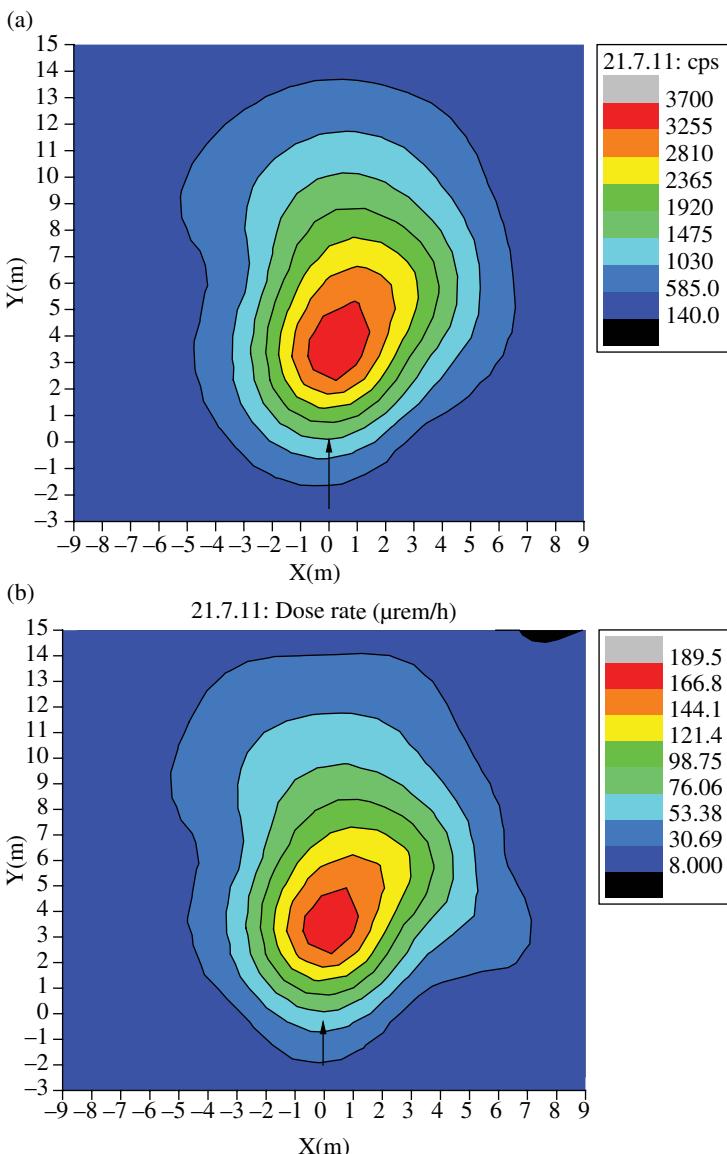


**FIGURE 7.7** The IDF CBRN building where the “Red House” experiment was conducted.

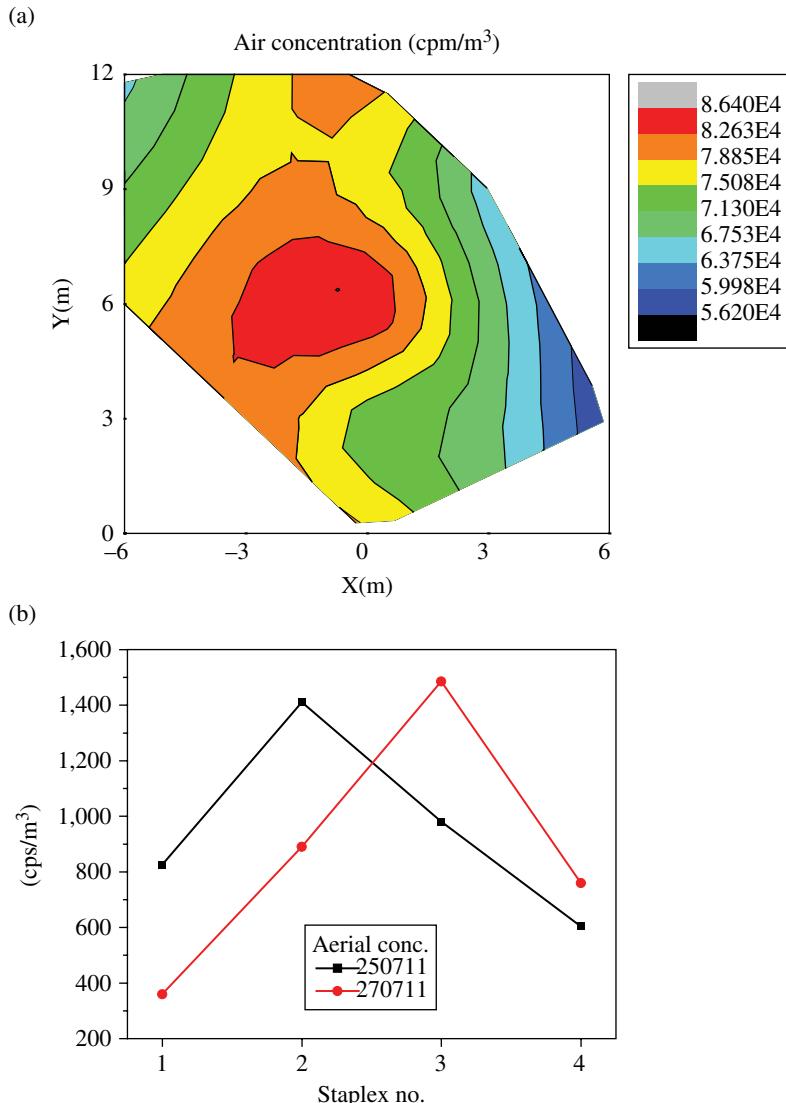
The radioactive concentration in the air inside the building was measured by 10 low volume (2 l/min) air samplers and 5 high volume air samplers (<http://www.staplex.com/airsamplers/TFIA/index.html#TFIA>) ( $20\text{ m}^3/10\text{ min}$ ). PDS and  $\text{LaBr}_3$  detectors were used for mapping the contamination level, both on the first and second floors. In order to ease the data analysis, the main hall of the first floor was gridded into 7 by 7 grid points (49 points). The size of a unit cell was 3 by  $3\text{ m}^2$ . Each grid point was coordinated by  $(x, y)$ , where the  $x$  coordinate was in the range of  $(-9, 9)\text{ m}$  and the  $y$  coordinate was in the range of  $(-3, 15)\text{ m}$ . Background readings were taken before each test inside and outside of the building. The results of these tests were subtracted from the measured value after the test.

The experiment included three repetitions of release. All of them were conducted from the second floor, from the following points: first release  $(0, 0)\text{ m}$ , second release  $(0, 12)\text{ m}$ , and third release  $(6, 6)\text{ m}$ . The dispersion was performed by an electric sprayer, which can produce fine particles in an order of several microns. Each dispersion included 50 mCi of  $^{99\text{m}}\text{Tc}$  mixed with 3.51 of water. The liquid drop size distribution was Gaussian shaped with a mean value of  $30\text{ }\mu\text{m}$  and a standard deviation of  $10\text{ }\mu\text{m}$ . The time period for each release was 10 min. Upon spraying, the aerosol was dispersed by the building ventilation system. The aerosol was anticipated to dry in a short time period leaving a small micrometer size salt particle containing  $^{99\text{m}}\text{Tc}$ .

A typical spatial distribution of the floor surface deposition, depicted in counts per second (cps) and in  $\mu\text{rem}$  per hour ( $\mu\text{rem}/\text{h}$ ), as measured in one of the tests is presented in Figure 7.8a and b, respectively. The spatial distributions of the air concentrations ( $\text{cps}/\text{m}^3$ ) at 1 m height, as measured at the first and second floor in one of the tests, are shown in Figure 7.9a and b, respectively.



**FIGURE 7.8** Spatial distribution of the floor surface deposition in (a) cps and (b)  $\mu\text{rem}/\text{h}$ .



**FIGURE 7.9** Air activity concentrations ( $\text{cps}/\text{m}^3$ ) at a height of 1 m, as measured at the (a) first and (b) second floor.

The quality of the outer filters located on the roof of the building determines the fraction of the total airborne material that is captured by them when the air ventilation system is working. Cumulative radiation measurements were therefore taken from the air ventilation system outer filters and at a distance of 1 m from them. Both measurements, taken about 40 min after each release, showed that most of the

radioactive material was stopped by the filters. It should be remembered that the air exchange rate inside the building during the tests was 8–12 cycles per hour. This means that 40 min after the release, at least five full air cycles passed through the filters before this measurement.

The meaning of this result is that the HEPA filters (<http://www.flanders-csc.com/hepa.htm>) located in the outer part of the air ventilation system ducts stop most of the radioactive particles carried by the air. Hence, the recommendation that can be made at this point is not to turn off the air-conditioning system after a radiological event inside a building. In this way, most of the air contamination will be captured by the filters, which can be replaced. Based upon these results, it is also highly recommended to install a radiation detector inside the ventilation system ducts in order to get fast alert for the existence of radioactive material inside the building.

### 7.3 DISCUSSION AND CONCLUSIONS

Based on the experimental results presented in this work and on other theoretical (Durante and Manti 2002; Elliott 2006; Slater et al. 2003; Tu 1999) and experimental (Cao et al. 2010; Harper et al. 2007; Musolino and Harper 2006; Prouza et al. 2010a, 2010b; Reshetin and Regens 2005; Sohier and Hardeman 2006) works conducted in the past, some new insights regarding the security of critical transportation systems can be obtained.

As demonstrated in the Goiania accident (IAEA 1988), a detonation of an RDD or a silent dispersion of radioactive material inside an airport terminal, train station, bus central station, subway system, or harbor (Zaidi 2007), even when a category 1 radiation source is used (IAEA and Bolshov 2006), will only cause minor injuries and few casualties from high radiation doses. On the other hand, this event will probably have a huge economic impact on the country involved (Schmid 2009) and therefore cannot be ignored.

A coordinated radiological terror attack on all of the international airports or main harbors or on a major transportation infrastructure like the train, bus, or subway system will probably close these facilities for periods of months or more, paralyzing passenger and merchandise movement through them, resulting in a big economic and physiologic effect (Eraker 2004). This long time period is needed for cleaning of the radioactive contamination to a point where these systems can be reopened according to IAEA guidelines for contaminated areas (IAEA 2004b). A very-small-scale demonstration on the large economical and psychological effect of the detection of radioactive contamination in an infrastructure system can be learned from the 2006  $^{210}\text{Po}$  incident (Cornett et al. 2009), where very small contamination areas were identified in parts of several hotels, restaurants, and offices and in the transportation system of London. Following this incident that was dangerous only to the person involved (Alexander Litvinenko (McFee and Leikin 2009)), several thousand people from all over the world went through a long screening process, from which only 168 were found contaminated with low but measurable levels of inside contamination (Maguire et al. 2010).

Additional general conclusions about the physical outcome of such events can be drawn from the experimental work presented here. First, it is clear that in a silent radiological event or in an RDD event where only a small quantity of explosives is involved, most of the radioactive material will be found in a close vicinity to the point of detonation or dispersion, resulting with high levels of contamination. The rest of the material will be found inside the ventilation system, especially on the surface of the filters, and will be carried by people to other parts of the infrastructure involved or outside. In an RDD event that involves a large quantity of explosives, the damaged and contaminated central area will be larger, the radioactive material concentration inside the affected area will be lower, and the area that will be contaminated with very low but still significant levels of radioactive contamination will be much larger and mostly downwind from the detonation point.

The big question that has yet to be answered is: **what has to be done in order to minimize the chances for such an event to occur in one of the critical transportation infrastructures around the world?**

The most promising answer to this question is based on the multilayer security system approach (Becker and Smit 2005; Haveman and Shatz 2006). The first security layer is a personal screening process of people at the entrance to the main infrastructure transportation facility. This process is not simple to perform; in order to achieve a 100% screening coverage, all entrances must be secured by trained security teams having monitoring capabilities, which will allow them to hold everyone who enters the facility for a short screening procedure, after which the person is either allowed to enter into the facility or he has to go through a more comprehensive screening process. If an international airport will be taken as an example, all private vehicles entering the airport from any point of entry and all of the people coming via public transportation system (buses, trains, subway) have to be stopped for a short questioning process before they are allowed to enter into the main airport area.

The second security layer, which has to be integrated into the security system, is an explosive detection system (Bruschini 2001). These systems are usually based on well-known techniques, and they can prevent conventional as well as RDD terror attacks or at least stop them at the entrance to the secured area.

The third security layer is one that can cope directly with any radiological terror threat (Kouzes 2009). The most common radioisotopes that can be used by terrorists for this purpose are listed in Table 7.1. From these isotopes, the most challenging ones are the alpha (Yaar et al. 2008) and beta (Yaar and Hussein 2004) emitters. A detection system that will identify these radioisotopes will easily detect gamma emitters like  $^{60}\text{Co}$ ,  $^{137}\text{Cs}$ , and  $^{192}\text{Ir}$ . The detection system can be a simple handheld radiation detector, operated by the security personnel posted at the first or second security layer, or a more complicated radiation detection portal suitable for the detection (and in some types identification) of radioactive material (Yaar and Peysakhov 2013; <http://www.airport-technology.com/features/feature124795>). The screening of public vehicles and cargo for radioactive material will result in some level of false-alarm rate coming from the presence of naturally occurring radioactive material (NORM) and from

people that had been treated or examined with radioisotopes several days before they went through the radiation detection portal (Kouzes and Siciliano 2006).

The security system described in the previous sections is aimed at prevention from a terrorist to enter into any transportation system carrying a radioactive material. If this system fails to alert, a second line of radiation detectors, aimed at detecting and/or identifying radioactive material release, has to be installed inside the facility. According to the results obtained in the RH experimental program, the preferred place for the positioning of these detectors is inside the air-conditioning ducts, as close as possible to the filters of the air that is being sucked from the building, and some other detectors have to be positioned outside the building in order to detect a release of radioactive material outside. The main purpose of this second line of radiation detectors is to raise an alert as soon as possible on the presence of radioactive material, in order to minimize the exposure of people involved and to prevent further transportation of the contamination to other parts of the infrastructure that was attacked and to other parts of the transportation system.

## 7.4 SUMMARY

The outcome of an accidental release of radioactive material in an urban environment is given together with the description of a comprehensive experimental program aimed at measuring the consequences of an RDD or a silent dispersion of radioactive material by terrorists. The results obtained in this experiment program, together with other experimental and theoretical results obtained by others, are used in order to draw a basic outline for a system that can lower the possibility and minimize the outcome of such an event in any critical transportation system. The implementation of these recommendations in the transportation systems is not simple due to the system's high installation and operating costs and its disturbance to the movement of passengers and goods. It is in the hand of decision makers to decide whether they prefer to enhance the preparedness of our critical transportation systems in order to prevent a possible radiological terror event, in spite of the extra cost and delays that these reinforced security steps will probably cause.

## REFERENCES

- J.M. Acton, M.B. Rogers, and P.D. Zimmerman, Beyond the Dirty Bomb: Re-thinking Radiological Terror, *Survival: Global Politics and Strategy*, 49 (2007) 151.
- J. Becker and L. Smit, *Transport Security, Annex XVIII of ASSESS Final Report*, DG TREN, European Commission, Brussels (2005).
- International Atomic Energy Agency and L.A. Bolshov, Objective and Subjective Impediments to the Broad and Successful Application of Ionizing Radiation Sources, in *Safety and Security of Radioactive Sources: Towards a Global System for the Continuous Control of Sources Through Their Life Cycle*, Proceedings of an International Conference Held in Bordeaux, June 27–July 1, 2005, International Atomic Energy Agency, Vienna (2006), p. 283.

- C. Bruschini, Commercial Systems for the Direct Detection of Explosive for Explosive Ordnance Disposal Tasks, *Subsurface Sensing Technologies and Applications*, 2 (2001) 299.
- X. Cao, G. Roy, P. Brousseau, L. Erhardt, and W. Andrews, A Cloud Rise Model for Dust and Soot from High Explosive Detonations, *Propellants, Explosives, Pyrotechnics*, 35 (2010) 1.
- J. Cornett, B. Tracy, G. Kraner, J. Whyte, G. Moodie, J.P. Auclair, and D. Thomson, Polonium-210: Lessons Learned from the Contamination of Individual Canadians, *Radiation Protection Dosimetry*, 134 (2009) 164.
- M. Durante and L. Manti, Estimates of Radiological Risk from a Terrorist Attack Using Plutonium, *Radiation Environment Biophysics*, 41 (2002) 125.
- W.C. Eckelman, Unparalleled Contribution of Technetium-99 m to Medicine Over 5 Decades, *JACC: Cardiovascular Imaging*, 2 (2009) 364.
- A. Elliott, Security of Radioactive Materials for Medical Use, in S. Apikyan and D. Diamond (eds.), *Countering Nuclear and Radiological Terrorism*, Springer, Dordrecht (2006) 95.
- E. Eraker, Cleanup After a Radiological Attack, U.S. Prepares Guidance, *The Nonproliferation Review*, 11 (2004) 167.
- F.T. Harper, S.V. Musolino, and W.B. Wente, Realistic Radiological Dispersal Device Hazard Boundaries and Ramifications for Early Consequence Management Decisions, *Health Physics*, 93 (2007) 1.
- J.D. Haveman and H.J. Shatz (eds.), *Protecting the Nation's Seaports: Balancing Security and Cost*, PPIC Publications, San Francisco, CA (2006).
- International Atomic Energy Agency, *The Radiological Accident in Goiania*, International Atomic Energy Agency, Vienna (1988).
- International Atomic Energy Agency, *Code of Conduct on the Safety and Security of Radioactive Sources*, International Atomic Energy Agency, Vienna (2004a).
- International Atomic Energy Agency, *Remediation of Sites with, Dispersed Radioactive Contamination*, Technical Reports Series No. 424, International Atomic Energy Agency, Vienna (2004b).
- International Atomic Energy Agency, *Categorization of Radioactive Sources*, IAEA Safety Standards for Protecting People and the Environment, Safety Guide No. RS-G-1.9, International Atomic Energy Agency, Vienna (2005).
- International Atomic Energy Agency, *Manual for First Responders to a Radiological Emergency, EPR-First Responders*, International Atomic Energy Agency, Vienna (2006).
- R.T. Kouzes, Challenges for Interdiction of Nuclear Threats at Borders, in First International Conference on Advancements in Nuclear Instrumentation Measurement Methods and their Applications (ANIMMA), Marseille, June 7–10 (2009) 1.
- R.T. Kouzes and E.R. Siciliano, The Response of Radiation Portal Monitors to Medical Radionuclides at Border Crossings, *Radiation Measurements*, 41 (2006) 499.
- J.O. Lubenau and D.J. Storm, Safety and Security of Radiation Sources in the Aftermath of 11 September 2001, *Health Physics*, 83 (2002) 155.
- H. Maguire, G. Fraser, J. Croft, M. Bailey, P. Tattersall, M. Morrey, D. Turbitt, R. Ruggles, L. Bishop, I. Giraudon, B. Walsh, B. Evans, O. Morgan, M. Clark, N. Lightfoot, R. Gilmour, R. Gross, R. Cox, and P. Troop, Assessing Public Health Risk in the London Polonium-210 Incident, 2006, *Public Health*, 124 (2010) 313.
- G. Makinen, *The Economic Effects of 9/11: A Retrospective Assessment*, Report for Congress, RL31617, Congressional Research Service, The Library of Congress, Washington, DC (2002).

- R.B. McFee and J.B. Leikin, Death by Polonium-210: Lessons Learned from the Murder of Former Soviet Spy Alexander Litvinenko, *Seminars in Diagnostic Pathology*, 26 (2009) 61.
- P. Murphy, *Intelligence and Security Committee Report into the London Terrorist Attacks on 7 July 2005, ISC 105/2006*, The Stationery Office, Norwich (2006).
- S.V. Musolino and F.T. Harper, Emergency Response Guidance for the First 48 Hours after the Outdoor Detonation of an Explosive Radiological Dispersal Device, *Health Physics*, 90 (2006) 377.
- Office of Intelligence and Analysis, The Terrorist Threat to the U.S. Commercial Passenger and Freight Rail System, Office of Intelligence and Analysis/Directorate for Preparedness, Homeland Infrastructure Threat & Risk Analysis Center (2006). <http://www.dhs.gov/about-office-intelligence-and-analysis> (accessed March 1, 2015).
- Z. Prouza, V. Beckova, I. Cespirova, J. Helebrant, J. Hulka, P. Kuca, V. Michalek, P. Rulik, J. Skrkal, and J. Hovorka, Field Tests Using Radioactive Matter, *Radiation Protection Dosimetry*, 139 (2010a) 519.
- Z. Prouza, J. Helebrant, V. Beckova, I. Cespirova, J. Hulka, P. Kuca, V. Michalek, P. Rulik, and J. Skrkal, Explosion Tests Using Radioactive Substances, in Proceedings of Third European IPRA Congress, Helsinki, Finland, June 14–16, 2010b.
- F. Reinares, The Madrid Bombing and Global Jihadism, *Survival: Global Politics and Strategy*, 52 (2010) 83.
- V.P. Reshetin and J.L. Regens, Estimation of Radioactivity Levels Associated with a <sup>90</sup>Sr Dirty Bomb Event, *Atmospheric Environment*, 39 (2005) 4471.
- A.P. Schmid, The Ultimate Threat: Terrorism and Weapons of Mass Destruction, *Global Dialogue*, 2 (2000) 1.
- A.P. Schmid, High Consequence Radiological Terrorism Scenarios—U.N., in W.D. Wood and D.M. Robinson (eds.), *International Approaches to Securing Radioactive Sources against Terrorism*, Springer, Dordrecht (2009) 79.
- A. Sharon, I. Halevy, I. Sheleg, R. Yanush, D. Sattinger, U. Admon, and I. Yaar, Evaluation of the Fraction of Material Emitted after an Indoor Explosion from Building Openings, Analysis According to the Results Obtained in the GF-7 Experiment, NRCN Report, N10/006. Nuclear Research Centre Negev (NRCN), Beer-Sheva (2010).
- A. Sharon, I. Halevy, Z. Bernstein, M. Levy, S. Tabibzada, A. Ashkenazi, and I. Yaar, *The “Red House” Project, An Experimental Study of Indoor Dispersion of Radioactive Material*. NRCN Private Communication. Nuclear Research Centre Negev (NRCN), Beer-Sheva (2011).
- A. Sharon, I. Halevy, D. Sattinger, and I. Yaar, Cloud Rise Model for Radiological Dispersal Device Events, *Atmospheric Environment*, 54 (2012a) 603.
- A. Sharon, I. Halevy, Z. Berenstien, P. Banaim, and I. Yaar, “Green Field III”—November 2012 Campaign, Preliminary Summary, NRCN Report, N972/0113. Nuclear Research Centre Negev (NRCN), Beer-Sheva (2012b).
- C.O. Slater, J.C. Gehin, and R.T. Santoro, *A Study of the Effects of a Radiation Dispersal Device*, ORNL/TM-2003/128, Oak Ridge National Laboratory, Nuclear Science and Technology Division (94), Oak Ridge, TN (2003).
- A. Sohier and F. Hardeman, Radiological Dispersion Devices: Are We Prepared? *Journal of Environmental Radioactivity*, 85 (2006) 171.

- A.T. Tu, Overview of Sarin Terrorist Attacks in Japan, in A.T. Tu and W. Gaffield (eds.), ACS Symposium Series, Vol. 745, *Natural and Selected Synthetic Toxins*, American Chemical Society, Washington, DC (1999) 304–317.
- I. Yaar and E.M.A. Hussein, Passive Detection of Concealed 90Sr RTGs in Transport, *Packaging, Transport, Storage and Security of Radioactive Material* 15 (2004) 149.
- I. Yaar and I. Peysakhov, A Multiple-Detector Radioactive Material Detection Spectroscopic (RMDS) Portal, *Nuclear Instruments and Methods in Physics Research A*, 712 (2013) 62.
- I. Yaar, I. Peysakhov, and E.M.A. Hussein, Passive Detection and Identification of a Concealed 241Am Source in Transport, *Packaging, Transport, Storage and Security of Radioactive Material*, 19 (2008) 189.
- M.K. Zaidi, Risk Assessment in Detection and Prevention of Terrorist Attacks in Harbors and Costal Areas, in I. Linkov, G.A. Kiker, and R.J. Wenning (eds.), *Environmental Security in Harbors and Coastal Areas*, Springer, Dordrecht (2007) 309.
- P.D. Zimmerman and C. Loeb, Dirty Bombs: The Threat Revisited, *Defense Horizons*, 38 (2004) 1.



## **SECTION II**

---

### **SECURITY CONSIDERATION FOR MODES OF TRANSPORTATION**



---

# 8

---

## SECURING PUBLIC TRANSIT SYSTEMS

MARTIN WACHS<sup>1</sup>, CAMILLE N.Y. FINK<sup>2</sup>,  
ANASTASIA LOUKAITOU-SIDERIS<sup>1</sup>, AND BRIAN D. TAYLOR<sup>1</sup>

<sup>1</sup>*Department of Urban Planning and Institute of Transportation Studies, Luskin School of Public Affairs, UCLA, Los Angeles, CA, USA*

<sup>2</sup>*American Planning Association, Chicago, IL, USA*

### 8.1 INTRODUCTION: THE CHALLENGE OF TRANSIT SECURITY

Public transportation systems are attractive targets for would-be terrorists trying to inflict harm and maximize disruption (Balog et al. 2002). Public transit, including bus systems, urban metro and light rail systems, and commuter rail lines, have all been targeted hundreds of times over the last three decades by domestic and international terrorists and criminals (Federal Transit Administration 2004). This chapter provides a brief overview of the types, incidence, and characteristics of terrorist acts against transit. It then discusses a variety of transit security strategies, including policing, surveillance and communications technologies, training programs, coordination strategies, and environmental design. Because it is often logical to combine antiterrorism and anticrime strategies, we also examine the compatibility between such strategies. This chapter draws from our previous work on transit security (Fink et al. 2005; Taylor et al. 2005; Loukaitou-Sideris et al. 2006; Cherry et al. 2008) and has been updated based on recent interviews with transit security experts from the American Public Transportation Association (APTA) and the Federal Transit Administration (FTA) in the United States and L'Union Internationale des

Transports Publics (UITP, also known as the International Association of Public Transport) based in Brussels, Belgium.

Transit serves very large numbers of people over extensive networks of stations, stops, and facilities in cities around the globe. The openness of transit systems, the availability of information about operations, and the anonymity of passengers are necessary to the successful operation of systems yet lead to their being inherently vulnerable. It is not only possible but relatively easy for potential terrorists to find information useful for planning attacks against transit systems and to hide in crowds of transit travelers without arousing suspicion. Securing such open and public systems presents a series of problems. While the volume of passengers and variety of operating environments provide myriad opportunities for those who wish to cause harm, it also makes it impractical for transit operators to instigate many of the security tactics employed, for example, in commercial aviation (Jenkins 2001).

On the other hand, while there are hundreds of billions of transit trips annually across the globe, only a handful of transit terrorist attacks have taken place in any given year, and these have usually occurred within contexts of political instability and unrest. The chances of a transit traveler being victimized by an act of terrorism are infinitesimally small, even on a crowded rail system in a high-risk region of the world. This is just one of many factors making transit security enormously challenging. It is impossible and illogical to provide a high level of security everywhere and at all times on public transit systems, while the consequences of a single attack can be dramatic and costly. Indeed, comprehensive, invasive preventive security measures on public transit, such as the screening of passengers and luggage with X-ray machines and metal detectors, hand searches, passenger profiling, sniffer dogs, and/or patrols by armed guards, would almost certainly lead to intolerable delays for passengers and unacceptable costs to transit agencies. Intrusive security measures would substantially increase cost per trip and the price or subsidy needed for transit. It would be costly to service providers and inconvenient to passengers, and shift travelers and cities toward greater dependence on private automobiles. Indeed, travel in large cities would change forever should open, accessible transit systems become “secured” (United States General Accounting Office 2002). Although airport-style screening is not feasible, new technologies do offer potential alternatives for transit agencies. Some of the most widely discussed developments include “smart” or “intelligent” video analytics; electronic, chemical, or radiological sensors and detection systems; and other portable or handheld screening devices (TCRP 2007; Schulz and Gilbert 2011).

## 8.2 TYPOLOGY OF TRANSIT TERRORISM

Some well-publicized and deadly bombings of public transit systems have put transportation officials around the world on edge. Stations, buses, and trains in London, Madrid, Moscow, Paris, Tokyo, and dozens of other cities have been the

sites for terrorist attacks in recent years. These attacks, quite understandably, have prompted calls for increased efforts to make public transit systems safe from terrorists. Such calls assume, of course, that public transit and transportation and infrastructure systems more broadly are the foci of the problem and appropriate venues for policy-making and action.

Acts of terrorism intersect with transportation systems in three ways:

1. When transportation is the *means* by which a terrorist attack is executed
2. When transportation is the *end*, or target, of a terrorist attack
3. When the *crowds* that many transportation modes generate are the focus of a terrorist attack

Examples of transportation as the *means* of a terrorist attack include the use of automobiles, buses, or trains to convey explosives or act as weapons—as happened in the September 11, 2001 attacks on New York City and Washington, DC. Examples of transportation as the *ends* of a terrorist attack include attacks on bridges or tunnels to disrupt transit, railroad, or highway operations, exact economic costs (but not necessarily human casualties), and attract attention; this describes the Irish Republican Army bombing campaign against transit targets in England and Northern Ireland between the early 1970s and mid-1990s. In each of these cases, the unique characteristics of transportation (and other infrastructure) networks define many aspects of the attacks, emergency response, and system protection. In recent years, transportation systems have also faced the possibility of being victimized through cyberattacks, which can disrupt their operations by affecting information flows needed to manage system operations (Radatti 2008; Fries et al. 2009). In all of these cases, the physical design of the vehicles, rights-of-way, stations, and platforms, as well as computer systems and monitoring and surveillance of the system, must be executed in a particular transportation context.

When *crowds* are the targets of the terrorists, which has most often been the case in recent suicide bomb attacks, defining the problem and its solutions in terms of transportation is more problematic. While public transit was the venue in the sarin gas attack on the Tokyo subway and the more recent random shooter attack in Mumbai, it was concentrations of people—and not the transit system per se—that most likely attracted the terrorists. Some aspects of transportation system design, like tunnels in which people are concentrated, can heighten the attractiveness of transit venues for those bent on attacking crowds. Airports, rail stations, and bus and ferry terminals all concentrate large numbers of people in small, often enclosed spaces, making them attractive targets for terrorists. Such crowding is not unique to transportation stations and terminals however. Skyscrapers, shopping malls, concerts, and sporting events likewise assemble large numbers of people in small spaces—as do major celebrations, parades, and religious convocations. Even if it were possible to completely close and secure public transit systems attractive to terrorists because of the crowds they generate, there would remain a considerable number of potential venues for devastating attacks on large crowds of people. Thus,

one cannot assume that securing public transit systems from terrorists in search of crowds in enclosed spaces would end or even mitigate such attacks. Some theorists argue that securing an environment can simply “displace” criminal or terrorist activities to other locations.

### 8.3 INCIDENCE OF TRANSIT TERRORISM

While the threat of transit terrorism has been felt more sharply in recent years, terrorist acts against transit systems are not only a recent occurrence. Much of the international terrorism policy literature does not dwell on transportation terrorism, and most of the latter addresses aviation and cargo movement, despite the fact that mass transit is clearly a target and carries more passengers annually than air transport. For example, a 2000 article in *TR News*, published by the Transportation Research Board with the auspicious title “Transportation Security: Agenda for the 21st Century,” made no mention of rail transit security issues (Morgan and Abramson 2000). Nonetheless, many urban areas’ transit systems and police departments have heightened security planning efforts in response to high-profile, albeit rare, rail transit terrorist attacks in Madrid in 2004, Mumbai in 2008, and Moscow in 2004 and 2010, as well as in London, Paris, and Tokyo. Bus bombings in Israel, India, and elsewhere have further elevated concerns.

But what exactly is transit terrorism? One useful definition is offered by the US Federal Bureau of Investigation (FBI). The FBI’s official definition of terrorism is laid out in the Code of Federal Regulations as “a violent act or an act dangerous to human life, in violation of the criminal laws of the United States or of any state, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social goals” (Federal Bureau of Investigation 1999, ii). By this definition, terrorism is not limited to plots by extranational organizations. According to data from the National Consortium for the Study of Terrorism and Responses to Terrorism (START), there were 2608 terrorist attacks in the United States from 1970 to 2011. These attacks were perpetrated by an extremely diverse array of organizations and individuals, in support of many different agendas including ethnonationalist separatism, antigovernment extremism, environmentalism, and neo-Nazism (LaFree et al. 2012). Although urban rail transit has not been a primary target of these groups, the 1995 derailment of Amtrak’s Sunset Limited cross-country passenger train in the United States by right-wing militants drew attention to the threat of such attacks. Because transit agencies are more concerned with the effects of attacks, rather than motivations for them, security efforts also focus on acts by deranged individuals, such as in the case of the 1994 Fulton Street firebombing in the New York City subway (Boyd and Sullivan 1997). While not technically terrorism as defined by the FBI, bomb threats and acts of mass violence intended to further personal rather than political goals are no less crippling to transit systems than are politically motivated attacks.

In addition to defining terrorism, it may be equally difficult to simply define “transit,” since transportation services vary greatly by mode, purpose, and type or class of service. The vast majority of transit passengers worldwide travel on buses, but light rail (trolleys, trams), heavy rail (metros), and marine ferries constitute important elements of many urban transportation systems, especially in large cities. Longer distance bus, commuter, and intercity rail operations often travel on the same streets and tracks as do more local transit services, frequently serving the same stops and stations. Since bus and rail transit modes often overlap, many police agencies have undifferentiated responsibility for all of them.

Jenkins and Butterworth’s (2010) research sheds light on the nature of terrorist threats facing transit systems. Their work—which examines both rail and bus transit operators—comprises 1633 separate incidents of terrorist attacks and other “significant criminal incidents” from 1920 through 2010 involving public transportation, culled from numerous public sources and databases, including the Global Terrorism Database by the START, the RAND Corporation, and the FTA and Transportation Security Administration (TSA) chronologies.

According to Jenkins and Butterworth (2010), the vast majority of transit terrorist acts occurred since 1970, and their frequency and lethality increased through 2008, but then decreased significantly during the last two years of their analysis. About half of the recorded incidents involved bus transit, just over 40% rail, and the remainder bridges, tunnels, or roads. Bombings were the most common mode of attack; 74% of the attacks involved explosive or incendiary devices. Other tactics included assaults with weapons, arson, armed hijacking, robbery, sabotage, kidnapping, and mortar attacks. The 1995 sarin gas attack on the Tokyo subway was the only incident of chemical or biological attack. However, that attack, which killed 12 people and injured thousands of others, prompted many transit systems in the industrialized world to include chemical or biological attacks in their security planning.

Jenkins and Butterworth (2010) find that the goal of most attacks against transportation systems is to kill rather than cause economic disruptions. Among the attacks analyzed, 38% resulted in at least one death, 17% in at least five deaths, and 9% in ten deaths or more. They note that attacks against trains—including attacks in Moscow, Mumbai, London, and Madrid—have been particularly deadly, resulting in more than 50 fatalities each. The 62% of attacks that did not result in deaths were either failed or thwarted attempts or were focused on causing disruptions to portions of the transportation system, such as tracks and roads.

An examination of 15 failed terrorist attacks against surface transportation systems also reveals some important aspects of these plots that can inform transit security planning (Jenkins and Trella 2012). While not comprehensive (the plots together represent an effort by jihadists to target sites in Western nations, including New York; Washington, DC; London; Milan; Cologne; Barcelona; Melbourne; and Sydney), the details of the failed plans suggest that attackers intended the incidents to result in the greatest possible lethality. While most of the plots involved bombs, several of the earlier plans involved chemical and biological materials. Jenkins and

Trella (2012) noted that most of the plots were thwarted in the early stages through the use of intelligence.

The spatial distribution of incidents reflects the geography of political volatility. Of all attacks targeting transportation systems, most have occurred in South Asia (32%), followed by the Middle East and North Africa (19%), Western Europe (13%), Southeast Asia (10%), Russia and the Newly Independent States (8%), South America (7%), and sub-Saharan Africa (5%). India, Israel, Pakistan, Russia, the Philippines, the United Kingdom, Colombia, Sri Lanka, and Turkey have suffered the greatest number of overall attacks. Accounting for the lethality of attacks—measured as fatalities per attack (FPA)—the rankings shift somewhat, with China, Sri Lanka, Italy, Algeria, and India (all but one of which are developing countries) having the highest FPA levels (Jenkins and Butterworth 2010).

## 8.4 SECURING TRANSIT FROM TERRORISM

Transportation, police, and intelligence agencies are all engaged in efforts to increase transit security. The strategies employed range widely from information gathering to dramatically improved surveillance techniques and include information sharing, staff training, and encouraged vigilance on the part of the traveling public. Some of these approaches are elaborated upon in this section. Organizations employing these strategies include international and national intelligence gathering organizations that collaborate with managers of local transit systems. The wide ranging participants in the provision of transit security also include national armies and localized and specialized transit police agencies that patrol stations and rail cars. Institutional responsibilities differ depending upon national and local cultures and customs, though over time collaborations are growing and communications among them are improving.

### 8.4.1 Transit Policing

Transit agencies have adopted a wide variety of policing arrangements, reflecting differences in local laws, history, and legislation. Transit systems can be protected by “sworn” transit law enforcement, nonsworn transit police (private security), contracted local police departments, a dedicated bureau of local law enforcement, no formal security (relying exclusively on law enforcement in the jurisdictions that host the systems), and, in the case of some European countries, even national military forces. In the United States, most agencies use a combination of policing options.

Major terrorist events have significantly affected policing strategies. The sarin gas attack in Tokyo and more recent attack in Madrid prompted transit security officials to step up patrols, warn passengers to report suspicious persons, and reduce personal and property crime in transit systems. Japanese transit operators hoped that potential terrorists would be dissuaded by the greater presence of security guards. While security officials believed the increased level of policing on their transit system had effectively reduced crime, they did not report as much certainty regarding its effect on terrorism prevention. According to an official from the Japanese Subway and

Streetcar Service Division of the Transportation Bureau, “It is really hard to claim that such patrolling efforts have paid off and have prevented terrorism in our system” (Taylor et al. 2005).

After the March 2004 attack in Madrid, Red Nacional de los Ferrocarriles Españoles (RENFE), Spain’s national train system intensified its existing security measures and adopted new ones. RENFE redeployed its police forces and directed them to focus on the safety of passengers, while intensifying their vigilance against suspicious persons. In conjunction with these efforts, the Spanish army for the first time began assisting in the policing of railway facilities. RENFE officials at the time described the coordination between army forces, municipal police, and RENFE security forces as good. At the Port Authority Trans-Hudson (PATH), whose system links New York City with suburban New Jersey, police responded to the Madrid attacks by using patrol tactics that included scrutinizing areas between parked rail cars and in station vestibules, as well as inspecting unoccupied rail cars at terminal stations. In addition, PATH started using more undercover police and flooding different parts of the system with police at varying times of the day and night (Taylor et al. 2005).

Policing by trained officers of the British Transport Police (BTP) is considered absolutely essential for the safe and secure operation of railways in Great Britain. The total, nationwide force in 2012 numbered about 2900 officers. In a 2004 interview, a BTP security official said that the British believe that having a force dedicated completely to transit security was advantageous as it provides consistency across the system and familiarity on the part of officers with issues and concerns that may be particular to Britain’s to transit systems (Taylor et al. 2005).

Passenger screening is a common terrorism suppression strategy, but the need to move large numbers of people through an open and accessible public transit network makes complete screening of all passengers unfeasible. A few examples of full passenger screening on intercity rail travel do exist, however: the Eurostar running between Britain and mainland Europe and systems in China, Israel, and Turkey. Random screening is typically a more practical strategy for urban transit systems and can both reassure passengers and deter would-be attackers. Technology for widespread screening is improving but has yet to be widely adopted for screening large numbers of passengers (Jenkins and Butterworth 2007), and in many cases, sniffing dogs used for explosive detection are considered more cost-effective than security screening technology (Mancini interview 2012).

#### **8.4.2 Surveillance and Communications Technologies**

Transit systems are by their nature physically expansive; thus, it is both logistically challenging and very expensive to patrol all parts of all facilities sufficiently to intercept and deter most terrorist acts. For this reason, surveillance technologies have been increasingly employed in lieu of human patrols over the past two decades. In earlier research, we found that over 90% of transit agencies in the United States responding to our survey had incorporated electronic communications upgrades and over 70% had video surveillance in their transit security programs (Taylor et al.

2005). These proportions are likely even higher today. Technological capabilities in the realm of transportation security are changing very rapidly, and it is anticipated that improvements in technology will continue to accelerate.

While it is critically important that trained and experienced personnel be in charge of security operations at all times, their reach and effectiveness can be extended dramatically by voice communications systems and video surveillance. Today, virtually every patrol officer and every transit vehicle operator in the developed world has voice communications capability with security personnel using lightweight and effective devices as simple as cell phones. The use of video surveillance cameras has become almost universal and has multiple benefits. Cameras have become more compact, cost-effective, and durable over time while achieving higher resolution. Urban transit buses often employ multiple cameras, and they are also widely deployed in urban and interurban rail systems. More sophisticated surveillance systems employ pattern and facial recognition software to assist with scans of large crowds. In older transit systems that contain many spaces difficult to observe by eye from central control points, electronic visual surveillance can be even more important. While some travelers find the surveillance cameras intrusive, others report feeling safer because they know that they and other passengers are being observed.

The Washington Metropolitan Area Transit Authority is an example of an agency that is especially security conscious, in part because of its location in the national capital. Its stations were designed and built to allow passive visibility of passengers by security personnel, yet the system recently upgraded its video surveillance system by adding or replacing more than 7000 cameras in just the rail portion of its system (Rothman 2012). While systems like the Washington Metro rely upon humans to monitor images captured by the electronic surveillance systems, software systems are being developed and deployed that assist with video surveillance by flagging suspicious human activity for investigation by security personnel.

The capability to use video technology is growing rapidly as behavior analytic and facial recognition software increases the utility of this technology. Extensive video surveillance combined with software analytics would allow transit operators to algorithmically profile behavior based on unusual activity. These systems would build upon large bodies of data to classify “normal” behavioral patterns for a given transit environment and thereby pick out exceptional activity such as unauthorized entry into secure areas or baggage left unattended (Schulz and Gilbert 2011). Facial recognition software could supplement these tools by scanning for suspected terrorists (Countermeasures Assessment et al. 2007). Such systems could have a wide reach and bring some welcome automated redundancies into practices that are currently labor and time intensive, particularly for busy, crowded transit hubs.

Transportation officials have also explored the possibility of embedding sensors into fare collection devices and ticketing machines. Various types of environmental monitoring or trace detection technologies could be used to investigate unusual biological, chemical, or electronic signals. Mobile devices could provide transit officers with even more flexibility in conducting patrols or investigations without bringing the operations of transit systems to a halt (Countermeasures Assessment et al. 2007).

These technologies are gradually becoming available and increasingly are being tested but have not seen widespread adoption thus far. A 2011 survey by the Transportation Research Board found that most transit agencies in the United States were still relying on fairly “low-tech” video surveillance despite the growing availability of sophisticated analytic tools (Schulz and Gilbert 2011). Barriers to adoption have included objections to invasions of personal privacy and other legal issues, reliability concerns, and costs of acquisition of the software and the associated costs of staff training. It is not easy for transit systems to determine in advance the effectiveness of new surveillance technologies, which is problematic because many of these new systems can be very costly to deploy. Thus, one of the most important functions of professional societies and consortia of transit organizations (discussed later in this chapter) has been information exchange and assessment of the performance of technology related to transit security.

#### 8.4.3 Training Programs for Security

A comprehensive security training program is an important component of security planning and incident response. UITP addresses training of frontline and supervisory employees, as well as those involved in security and policing. It defines roles, what to look for, and how to respond. Training typically includes interacting with passengers during an incident, conveying pertinent emergency and response information, and mitigating public alarm. The presence of identifiable and trained personnel helps an agency “reassure passengers as to its control over the transport network, enhancing trust and a sense of security” (UITP 2009, 42). The customizing and standardizing of security training for personnel at all levels of an agency can also improve coordination with police, fire, and intelligence officials in times of emergency.

The UITP describes the three “pillars” of security as (i) the human or “H” factor, meaning observant and committed staff and passengers; (ii) procedures, meaning response patterns that are understood and routinized by the agencies in charge; and (iii) technology, which refers to the increasing use of machines for surveillance to in turn free human observers for more sophisticated analytical responses. These elements combine to provide a comprehensive interlinked and interconnected security strategy. For example, technology alone does not provide the staff–passenger relationships crucial for an effective response plan: “Staff engaging with the passenger creates a sense of reassurance which cannot be fully achieved by technology. Customers want interaction with real people, either directly or through technological devices such as telephones and loudspeakers. Similarly only staff can provide direct help during incidents. For the H Factor to be most effective, staff must be qualified, trained, well-equipped and motivated” (UITP 2010, 2).

Security analysts agree that the vulnerability of transit systems to terrorist attacks should be reviewed periodically so security officials can refine training in response to evolving threats, such as the emerging cybersecurity threats. APTA in the United States offers peer review panels as part of its safety audit programs in order to help transit managers identify safety and security vulnerabilities in their systems and to develop effective response strategies. Relying upon knowledge of “best practices,”

these teams review existing training and staffing plans as well as manuals and operational procedures. Both the FTA and the Transportation Safety Institute (part of the U.S. Department of Transportation's Research and Innovative Technology Administration, or RITA) offer security training tools, including videos, courses, and publications (<http://transit-safety.fta.dot.gov/Security/TrainingTools/>; <http://www.tsi.dot.gov/>). Resource constraints can make follow-through and regular updates to training programs challenging for agencies. One strategy is to use technologies to extend and leverage limited training resources. Online training and webinars provide access to training resources beyond traditional classroom training (Gerhart interview 2012).

The European Commission has in place a Community Research and Development Information Service that includes a program called Secured Urban Transportation—A European Demonstration (SECUR-ED). SECUR-ED includes a comprehensive training package module along with identified best practices, procedures, and hardware and software modules. The goal is to bring together consultants and public transportation agency managers from across the European Union to develop common resources and training kits that include classroom, e-learning, simulators, and exercise delivery formats targeting frontline employees, security agents and managers, security and closed circuit television operators, and passengers (Maag 2012). Training topics include security and risk management in public transport, security operations and operations planning, conflict management, communication and cooperation, security practice, and emergency and crisis management (Maag 2012). These training and other modules are integrated through pilot programs into the networks of Madrid, Paris, Milan, and Berlin with later adaptations for the scaling of these resources to medium-sized and smaller agencies throughout the European Union.

#### **8.4.4 Information and Outreach Strategies**

The crime and public safety literature has for years suggested that public awareness of and involvement in crime reporting and prevention can greatly increase public surveillance and help reduce the acceptability of both petty and felonious criminal behavior (Jacobs 1961). Public education and outreach strategies are considered central to safety and security campaigns. Many transit systems in the United States and abroad have actively sought to enlist the help of patrons in watching for and reporting suspicious activity by text messaging, cell phones, and the use of telephones provided at stations and stops, and by reporting concerns directly to uniformed personnel.

Transit managers value customer feedback and a number have launched information and outreach campaigns to raise the vigilance of the public. On some systems, posters at the stations and stickers on train windows remind passengers to report any suspicious activity or unattended bags. In the United States, APTA and the TSA partnered with other agencies to develop a public awareness program to educate transit riders and employees on the importance of being alert and aware of

surroundings and reporting anything that appears suspicious. The program, still in operation, is called “Transit Watch,” and it has spurred other programs, such as the “If You See Something, Say Something” program of the New York City Metropolitan Transportation Authority.

Such programs are also widespread in Europe, but a UITP study found that their effectiveness depends on national culture (UITP 2009). For example, the British are open to the kind of participatory engagement and shared responsibility of public education campaign strategies. In Germany, however, this sort of “whistle-blowing” activity is frowned upon, and different approaches are needed. In Italy, this civic vigilance approach is not one that people respond to well, as the idea of protecting one’s individual family and friends is seen as most important. Campaigns in Singapore are very graphic, showing, for example, the consequences of what might happen if riders do not speak up about suspicious people or situations. The cultural diversity of Europe has required that campaigns be tailored to specific cultural norms and expectations (Mancini interview 2012).

Transit agency officials face numerous challenges in designing and implementing antiterrorism public education and outreach campaigns. On the one hand, an overly aggressive program could alarm and deter riders from using public transit. On the other, outreach to the community helps raise awareness about both terrorist and non-terrorist threats and issues, so this can help decrease crime and strengthen relations between the agency and the public. The content of an outreach strategy, therefore, is often matched to the risks and threats against specific targets and areas as well as the advantages and disadvantages of pursuing a program. However, the effectiveness of campaigns remains unclear. A 2010 examination of five transit security campaigns in the San Francisco Bay Area found that agencies did not attempt to gauge the effectiveness of their security awareness campaigns through outcome and output measures about changes in passenger behavior and understanding of transit security issues (Rohlich et al. 2010).

#### **8.4.5 Coordination and Information Sharing**

Rarely does a single public transit agency operate all service in a given metropolitan area, so interagency coordination—of planning, fares, service, and increasingly security—is a fact of life for most public transit managers. But interagency security coordination is different, in that it involves different types of agencies at different levels of government—police, intelligence agencies, industry groups, and so on—and not just other transit operators. For many public transit agencies, this type of multilevel coordination is relatively new.

Because the sizes and roles of public transit agencies vary so dramatically between the largest and smallest cities, the policing of transit systems varies substantially as well. Most small public transit systems simply rely on local police departments for protection against crime and security threats, with little active involvement from transit managers, particularly regarding questions of security. On the other hand, the largest transit operators typically either have their own

sworn police departments or contract with local police or sheriff's agencies for specialized transit police services. These larger agencies, which often manage rail and bus stations and exclusive rights-of-way in addition to vehicles, are both viewed as more likely terrorist targets and have longer histories of police and intelligence activities.

In addition to policing and surveillance, transit officials have devoted considerable time and effort over the past decade to improving the quality, timeliness, and dissemination of security intelligence to transit managers and those who police transit systems. In the 1990s and early 2000s, information sharing among transit and government security organizations was mostly unfamiliar territory, and many transit managers worried that they were not trusted by intelligence officials to handle sensitive information (Hull interview 2012). But the channels of communications and levels of trust among public transit operators and government security agencies have improved considerably in the 2000s; in the United States, this involves a variety of organizations, including the FBI; Department of Homeland Security, especially the TSA; and the Joint Terrorism Task Force (Hull interview 2012).

While there are sophisticated and articulated systems for intelligence sharing across national governments, there is not an analogous model for transit-specific security information sharing across government public transit organizations at the national level. Instead, most of the international coordination of intelligence and security best practices are handled by public transit industry groups, like the UITP, APTA, and the Collaboration of Railway Police and Security Services (COLPOFER) (Gerhart interview 2012; Hull interview 2012).

Increasingly, third-party intelligence services have been organized and deployed by transit industry organizations. In the European Union and the United States, the UITP and APTA have taken the lead in contracting with private security firms to organize, collect, and disseminate transit security intelligence on behalf of their member agencies. These organizations can do this because they have been given access to government security intelligence, which they customize for their members in the form of daily briefings and security alerts. These contract security services are provided by SecCom in Europe and through the Public Transit Information Sharing and Analysis Center in the United States (Hull interview 2012; Mancini interview 2012).

These contract security organizations—known colloquially as “ISACs” (for Information Sharing and Analysis Centers)—are not exclusive to public transportation; the US government has since the 1990s encouraged their development across a variety of industries, including financial services and information technologies. These various ISACs increasingly coordinate and share information among one another, bringing their particular industry focus to intelligence gathering and dissemination (Hull interview 2012). The most recent focus of ISACs has been on ways to protect their industry members from cybersecurity threats (Gerhart interview 2012; Hull interview 2012; Mancini interview 2012).

Efforts to improve interagency coordination have been enhanced in recent years through interagency security exercises, which participants report are both helpful in preparing for major security events, should they arise, and in gaining a better

understanding of the *modus operandi* of agencies with highly divergent missions and goals (Mancini interview 2012).

#### 8.4.6 Environmental Design

While the strategies discussed earlier rely on human or technological means to improve security, environmental design strategies are also very important. They have been used successfully for the prevention of transit crime (Felson 1996; La Vigne 1996), which is much more common than transit terrorism. Some of the principles behind environmental design strategies can also inform transit security strategies. At the same time, if strategies to reduce the likelihood and severity of transit terrorism also reduce the incidence of personal and property crimes on transit, such collateral crime benefits are likely to exceed the direct security benefits.

The principle that crime and the physical environment are related in systematic and controllable ways dates back half a century to Jane Jacob's (1961) calls for designs and mixed uses that facilitate more "eyes on the street." Eventually, design strategies aiming to reduce opportunities for crime and to discourage antisocial and criminal behavior became known as crime prevention through environmental design (CPTED). These strategies draw from Oscar Newman's (1972) concept of "defensible space"—an environment with physical characteristics that allow occupants to assume primary authority for ensuring their own safety. Defensible spaces usually exhibit three important characteristics: (i) territoriality, (ii) natural surveillance, and (iii) proper location. Territoriality is defined as "the capacity of the physical environment to create perceived zones of territorial influence" (Newman 1972, 50). According to Newman, individuals or groups with a sense of ownership or territory are more likely to protect "their" space against criminals. Thus, territorial strategies applicable to transit environments encourage occupants to take "ownership" of certain spaces and concentrate public uses and amenities to increase the likelihood that improper use of the space will not be tolerated by a critical mass of legitimate users.

Natural surveillance is defined as "the capacity of the physical environment to provide surveillance opportunities for residents and their agents" (Newman 1972, 50). Clear sightlines and unobstructed views of a space from its surroundings allow increased visibility by other users and from adjacent establishments and limit opportunities for criminal activities (Clarke 1983; Crowe 1991). This is illustrated in Figure 8.1.

Proper location involves the existence or proximity of "safe zones"—which are clean and well-maintained spaces. The idea is also echoed in the so-called "broken windows" theory, which asserts that well-maintained spaces send the message to potential criminals that inhabitants are in control and are likely to react if someone tries to violate this control and care. In contrast, as is apparent in Figure 8.2, the presence of unkempt physical environments with graffiti, litter, and "broken windows" (literally and metaphorically) encourages crime (Wilson and Kelling 1982).

The important role that environmental design plays in reducing or inviting crime in the transit environment is well documented. Studies indicate that the physical characteristics of stations such as open layouts, good lighting, fencing, and security hardware can reduce opportunities for crime (Felson 1996; LaVigne 1996; Harris



**FIGURE 8.1** Clear lines of sight from a surrounding establishment of a Stockholm tram stop (photo by Anastasia Loukaitou-Sideris).



**FIGURE 8.2** Litter in the vicinity of a Los Angeles bus stop (photo by Anastasia Loukaitou-Sideris).

1971; Ceccato 2011; Loukaitou-Sideris 2012). Design and landscaping elements can be utilized as a form of “soft control,” limiting access to particular spaces and facilities in station areas. For this reason, CPTED strategies are important parts of transit agencies’ crime prevention toolkits.

Some guiding principles and lessons of CPTED can inform antiterror security strategies, while others are less pertinent. In an environment as public and open as transit, some CPTED strategies are a countervailing force against more traditional target hardening or surveillance measures, which may interfere with an agency’s mandate to provide effective public transportation at an acceptable cost. Effective environmental design ensures that policing resources are used efficiently by making surveillance easier and reducing opportunities for terrorist acts—such as by eliminating places where bombs can be hidden or by erecting bollards to limit the passage of unauthorized vehicles into track and station areas but allow people to move about freely. Target hardening, by engineering blast resistance into existing transit facilities, may be too costly for the level of threat faced by even the most vulnerable transit systems, but more modest structural improvements to glazing or light fixtures can be more cost-effectively part of a system’s broader security strategy.

Design strategies for security can be incorporated into transit station design at three different times: (i) when constructing new stops and stations, (ii) when retrofitting older stops and stations, and (iii) after an incident or security breach (Yellow Design Foundation 2008). It is easier, more effective, and more cost-efficient to implement CPTED strategies in the process of station planning than after its construction. Transit systems now routinely incorporate CPTED strategies when building new stations or refurbishing old ones (Hull interview 2012). The FTA in the United States has established a safety and security certification process for capital improvement projects to which that agency contributes funds. Through this certification process, transit operators are held accountable to ensure that they incorporate CPTED concepts into the planning and designing of their facilities (Adduci et al. 2002; Hull interview 2012).

The FTA has also compiled a series of security-oriented design strategies for transit stations, summarized in Table 8.1 (Rabkin et al. 2004). These strategies operate in four different layers of a given facility: (i) layout and perimeter, (ii) interior, (iii) architectural and engineering features, and (iv) systems and services. Similar to personal and property crime prevention design strategies, such design strategies can also aim to reduce both the likelihood and impact of a terrorist attack. These include:

- “Hardening” the facility against a terrorist attack by making its structures more resilient to an attack
- Protecting valuable assets and facilities (e.g., operations control centers) by making them inaccessible behind gates and locks and “hiding” them behind multiple layers of secure spaces
- Incorporating redundancy by providing duplicate or varied functional spaces and backup systems (e.g., auxiliary control spaces)
- Minimizing the effects of an attack (e.g., incorporating fire suppression and ventilation systems, using noncombustible construction materials, eliminating sources of secondary fragmentation)

**TABLE 8.1 Security-Oriented Design Strategies for Transit Stations**

Design Feature	Type of Strategy	Goal	Effectiveness on Crime	Able to Retrofit
<i>Site Perimeter and Layout</i>				
Structures set back from roads	Access management	Deter/minimize		
Physical barriers (bollards, road spikes, fencing)	Access management	Deter/minimize	X	
Minimum number of vehicle entrances; size of other entrances	Access management	Deter	X	X
Prohibiting passage of vehicles	Natural surveillance	Deter/detect	X	X
Unobstructed sightlines toward station				
<i>Interior Layout</i>				
Transparency, unobstructed sightlines; minimum hidden areas/hiding places/remote passageways	Natural surveillance	Deter/detect	X	
Kiosks, ads, and information positioned to not disrupt sightlines	Natural surveillance	Deter/detect	X	X
Minimum use of columns, nook, and blind corners	Natural surveillance	Deter/detect	X	
Security mirrors on columns and corners	Natural surveillance	Deter/detect	X	
Strategic positioning of operator booths for maximum visibility	Natural surveillance	Deter/detect	X	In some cases
Critical assets buffered from public or vulnerable areas and secured with gates/locks	Target hardening/access management	Deter		
Nonpublic facilities hidden and not identified	Target hardening/access management	Deter	X	
Emergency evacuation routes/safe areas	Minimize			In some cases
<i>Architectural and Engineering Features</i>				
Bright paint colors to increase ambient lighting	Natural surveillance	Deter/detect	X	X
Minimum sources of secondary fragmentation (glass, vending machines, chairs, decorations)	Target hardening	Minimize	X	X
Vulnerable features designed to channel blasts	Target hardening	Minimize		
Shatterproof glazing	Target hardening	Minimize		X
Façade materials that resist explosive blasts	Target hardening	Minimize		
Noncombustible, fire retardant, nontoxic construction materials	Target hardening	Minimize		

<i>Systems and Services</i>						
Sufficient lighting/backup emergency lighting	Natural surveillance	Deter/detect	X			X
CCTV coverage of site perimeter and station	Surveillance	Deter/detect	X			X
Passenger scanners at entrances and appropriate surveillance at access points	Access management	Deter/detect	X			X
Close monitor of hiding places (trash cans, lockers, restrooms) for devices	Surveillance	Deter/detect	X			X
Motion detectors or intrusion alarms on vehicle entrances	Surveillance/access management	Deter/detect	X			X
Fire detection and suppression system	Target hardening	Detect/minimize	X			X
Chemical detection devices	Target hardening	Detect	X			X
Ventilation system/procedures for chemical/biological attacks	Target hardening	Detect/minimize	X			X
Communication links to administrative and emergency response centers	Communication	Detect/minimize	X			X
Call boxes, public address system	Communication	Deter/minimize	X			X

Adapted from Rabin et al. (2004, Table 6-2).

In newer transit systems, where CPTED methods have been employed in design and planning, video surveillance extends the capabilities of human observers and records observed activity that can be reviewed if suspicious incidents are reported.

Some CPTED design elements credited with combating crime can, in fact, become liabilities in the event of an incendiary attack. Both LaVigne (1996) and Boyd (1998) note the role of trash cans on Washington Metro station platforms in maintaining a clean environment where crime, littering, or related antisocial behavior are discouraged. This may be a good strategy in transit systems with low risk of terrorist attack, and trash cans and recycling bins are important passenger amenities. However, trash cans have also been used as delivery devices for terrorist bombings in transit stations and are frequently eliminated as an antiterror security strategy (Jenkins and Gersten 1997).

The use of glass as a design element is particularly problematic in the event of a bombing, but glass is cited by many as an effective means to discourage crime in transit environments by increasing both light and visibility (Felson 1996; LaVigne 1996; Myhre and Rosso 1996). Glass may enhance formal and informal surveillance by bringing in natural light, providing a sense of openness, and enhancing lines of sight. However, when ruptured by a bomb blast, glass can be extremely hazardous. Glass can be made safer by heat treating and lamination, which greatly reduce the number of large, dangerous shards when broken. But even if blast resistance is the only consideration (leaving aside aesthetics and building performance), decisions about glazing depend on many factors from the level of the bomb threat to the integrity of the supporting frame and to the blast load on the facility itself (American Institute of Architects 2003). Arguably, security cameras can provide better formal surveillance capabilities than glass with less liability, but in some instances, the use of glass increases visibility and thus improves the effectiveness of video surveillance. Cautions about the potential dangers of glass illustrate tensions among the design requirements of traditional crime security, antiterror security, and aesthetics—tensions that must be addressed and resolved in each specific design application.

## **8.5 COMPATIBILITY OF ANTITERROR AND ANTICRIME STRATEGIES**

Transit stations are frequently described as crime attractors (Brantingham and Brantingham 1993, 1995) because they concentrate large numbers of captive riders who become easy targets for crime. The existence of large crowds combined with the openness and accessibility of transit stations and predictability of transit routes and schedules makes transit stations desirable targets for pickpockets and muggers. For this reason, studies have repeatedly shown that fear of crime is a significant deterrent to transit use (Hartgen et al. 1993; Lynch and Atkins 1998). So while media and political attention have increasingly shifted toward protecting transit systems against terrorism, transit operators and passengers often worry even more about personal and property crimes on transit.

Given the recent security demands placed on transit managers, and the limited resources with which transit operators execute their most basic functions, efficiency and effectiveness must play a large role in any comprehensive approach to transit security. It thus makes sense to pursue a “dual-use” approach that protects systems against both terrorism and crime (Morgan and Abramson 2000; Goetz 2003). In many places, it has been difficult to justify the expenditures for securing a system against terrorism given the low incidence of terrorism and the variability of threat levels. Complementary security strategies that address other transit goals, like personal security from crime, are more likely to receive funding and support (Jenkins and Gersten 1997). Additionally, evidence suggests that travelers feel safer when a transit system is attentive to both types of security.

But how easy is it to integrate security from crime with security from transit terrorism? How compatible are measures that diminish opportunities for transit crime with measures that lessen the possibility of terrorist attacks against transit? The views of scholars on these questions are mixed. Some argue that “attack from criminal behavior or attack from terrorist activity only reflect a change in the level and types of threats. The process and challenges are the same” (Atlas 1999). In contrast, others warn that the “solution for a particular crime in a particular situation will not necessarily work for all types of crime” (Balog et al. 2003). We identified similar ambivalence among the transit professionals we interviewed in our earlier study on transit terrorism (Taylor et al. 2005). While some suggested that anticrime and antiterrorism efforts are not always reciprocal and complementary, others argued that such efforts can work hand in hand. The introduction of antiterrorist security measures into the Tokyo subway stations, for example, was associated with substantial reductions in robberies and thefts. Likewise, fewer crimes were reported in the period following the implementation of random parcel inspections in the Madrid metro system (Taylor et al. 2005). More recent interviews with transit industry representatives in the United States and Europe indicated a growing consensus that there is complementarity among anticrime antiterrorist strategies. For example, transit managers may install security technology in order to spot terrorist trespassers, but they will also get the added benefit of graffiti or theft reduction as a result of the greater surveillance (Mancini interview 2012).

Crime prevention strategies rely heavily on a thorough understanding of criminal motivation and behavior. A difference between criminals and terrorists, however, is that “ordinary” criminals are usually operating for personal gain, and their behavior is often rational and predictable. On the other hand, terrorists are more often motivated by ideological, political, or religious goals; their success relies on their ability to surprise, and their behavior is sometimes unpredictable as a result. For example, while ordinary criminals seek to evade capture, suicide bombers have no such concerns. Thus, a change in the level and type of threat can involve a significant alteration of practice for which some established crime prevention strategies may not be entirely suited.

The aforementioned differences notwithstanding, some transit crime and terrorism defenses share common objectives of natural surveillance and access control or access management. Thus, it is logical that some strategies that reduce the opportunity for

crime may also reduce the opportunity for terrorist activities. Natural surveillance refers to the ability of both legitimate users and security personnel to observe activity. Natural surveillance can be enhanced through design, such as the spatial layout of a station and building orientation. Similarly, access control can be achieved by using building or landscaping elements (walls, fences, bollards, landscaping) to limit or channel access to a facility. For example, using the principle of natural surveillance to limit opportunities to conceal illicit acts complements the common antiterrorist tactic of eliminating spaces where an attacker could conceal an explosive device. Similarly, using the principle of access control and management to eliminate the number of vehicle entrances to a station not only limits the potential destruction from car bombs but also thwarts an ordinary criminal's easy escape from the station after a crime. However, there is also the possibility that individual crime prevention strategies can conflict with the goals of designing against the threat of a terrorist attack. For example, anticrime strategies would suggest locating parking lots in close proximity to a station to facilitate casual monitoring of parked vehicles by staff and transit riders present at the station. However, allowing vehicles too close to a station building may increase its vulnerability to a car or truck bomb (Federal Emergency Management Agency 2003).

Looking specifically at transit stations, Table 8.1 lists 28 common design and building retrofit transit terrorism prevention strategies. Some have the goal of deterring or detecting impending terrorist acts, while others aspire to minimize the effect and damage from a terrorist act, should one occur. We can see that about half of these strategies are expected to reduce personal crime as well, primarily because they increase station visibility, enhance opportunities for natural surveillance, and/or minimize the possibility of a criminal's easy escape. On the other hand, antiterrorist strategies that focus on "target hardening"—making the facility more resilient to a terrorist attack—are not likely to have a major effect on transit crime.

Thus, while antiterrorism efforts may have the tangible benefit of reducing transit crime, it is important to consider the level of congruence of anticrime and antiterrorist strategies, which likely differ with the local situation and context. In spite of the risks of applying CPTED and other crime prevention strategies whole cloth to reduce the threat of terrorism, many guiding principles of and lessons of such strategies can inform antiterror security efforts. At the same time, it is important that security planners and designers first understand the nature of the threats posed by terrorists seeking large-scale destruction of transit facilities.

## 8.6 CONCLUSION

Transit security is an issue of importance and enormous complexity. To attract customers, transit systems need to create environments in which passengers feel safe from personal and property crime and from victimization by terrorists. Yet the smooth functioning of transit systems can be compromised by programs that aggressively promote security, and passengers can be hostile to intrusions into their normal commuting experience, largely because they assume that the probability of a terrorist

event is very low. Events that threaten this assumption are rare, but when they occur, the consequences for travelers and system managers are traumatic and long lasting.

Since the 1980s, approaches to the provision of security against terrorist attacks in transit systems have evolved considerably. From the early days during which emphasis was placed upon basic policing of transit systems and protection focused upon the hardening of potential targets, the approaches used today are more complex, sophisticated, and ultimately more cost-effective.

Basic policing of every transportation system remains important to maintaining efficiency in operations and is a critical element in responding to terrorist incidents (as well as crimes) when they do occur. Well-trained and effective police forces are central to effective transit system protection, but increasingly, they are augmented and complemented by many additional approaches.

Where new transit systems are constructed and when new stations are added to older systems or older facilities are renovated, they are increasingly designed with protection in mind. This includes designing for visibility and surveillance, and for improved circulation under stressful conditions, along with the use of construction materials and designs that minimize deaths and injuries if and when attacked. While passive approaches to security through environmental design are now routine when designing new systems or major renovations to physical facilities, many older systems continue to handle very large passenger volumes in facilities that were designed in some cases a century before these concepts came to the fore.

The physical design of the transit environment and the presence of traditional police forces are today widely complemented by technological devices, including cameras and voice communications systems, which have advanced dramatically over the past decade and today routinely provide security personnel with extended range and improved effectiveness.

To reduce the likelihood and impacts of terrorist attacks, transit systems need to make maximum use of physical design improvements, efficient policing, and dramatically improved technology for surveillance and communications. While such physical attributes are important parts of improved transit security, experience cited earlier indicates that intelligence operations are becoming far more effective than routine policing in the defeat of potential terrorist incidents. Since 2000, we have seen substantial progress in interagency collaboration across municipal and international boundaries in joint efforts to uncover plans to commit terrorist acts. So while designers and managers of transit systems consider every element of their system, they increasingly work collaboratively with law enforcement agencies and military and civilian intelligence agencies because information and monitoring suspicious behavior have proven an important complement to physical interventions.

Given limited financial resources, education and training of transit system staff and enhancement of passenger education and awareness are valuable complements to policing and antiterrorist intelligence work. Regular drills have been found to be cost-effective strategies, having some deterrence value and greater value in improving the effectiveness of respondents when incidents do occur.

The subject matter of transit security is inherently dynamic, responding to the changing nature of threats and taking advantage of the availability of new technology.

As an example, cybersecurity was not a significant element of transit system operations just a decade ago, but today, cyber terrorism is widely viewed as an important threat that requires new forms of training as well as investments in new software and technology. Beyond the scope of the present chapter is the response and recovery after terrorist incidents when they do occur in transportation environments; while we have focused here on prevention, many similar issues arise when agencies must respond quickly and effectively in emergency situations. Given the rapidity of change in planning for transit security and safety, transit industry leaders and managers must both enhance their own security efforts and continue to form partnerships with other transportation, security, and policing agencies in their regions and around the world.

## ACKNOWLEDGMENT

The authors are grateful to Chirag Rabari for the assistance he provided in finalizing the research presented in this chapter.

## REFERENCES

- Adduci, R.J., Boyd, A., and Caton, J. 2002. *Handbook for Transit Safety and Security Certification*. Washington, DC: US Department of Transportation.
- American Institute of Architects. 2003. *Security Planning and Design: A Guide for Architects and Building Design Professionals*. Hoboken, NJ: John Wiley & Sons, Inc.
- Atlas, R. 1999. *Is There a Difference in Designing for Crime or Terrorism?*. Miami, FL: Atlas Safety & Security Design, Inc. Available at: [http://cptd-security.com/atlas/index2.php?option=com\\_docman&task=doc\\_view&gid=36&Itemid=35](http://cptd-security.com/atlas/index2.php?option=com_docman&task=doc_view&gid=36&Itemid=35) (accessed on March 1, 2015).
- Balog, J.N., Devost, M.G., & Sullivan, J.P. 2002. *Communication of Threats: A Guide* (Transportation Cooperative Research Program Report 86). Washington, DC: National Academies Press.
- Balog, J.N., Boyd, A. and Caton, J. 2003. *Public Transportation System Security and Emergency Preparedness Planning Guide*. Washington, DC: Federal Transit Administration.
- Boyd, A. 1998. *Transit Security Handbook* Washington, DC: USDOT, Volpe National Transportation Systems Center.
- Boyd, A. and Sullivan, J.P. 1997. Emergency Preparedness for Transit Terrorism. In *TCRP Synthesis 27*. Washington, DC: National Research Council.
- Brantingham, P. and Brantingham, P. 1993. Nodes, Paths and Edges: Considerations on the Complexity of Crime and the Physical Environment. *Journal of Environmental Psychology*, 13: 3–28.
- Brantingham, P. and Brantingham, P. 1995. Criminality of Place: Crime Generators and Crime Attractors. *European Journal on Criminal Policy and Research*, 3(3): 1–26.
- Ceccato, V. 2011. *Safety in Stockholm's Underground Stations: The Importance of Environmental Attributes and Context*. Stockholm: Royal Institute of Technology.

- Cherry, C., Loukaitou-Sideris, A., and Wachs, M. 2008. Subway Station Design and Management: Lessons from Case Studies of Contemporary Terrorist Incidents. *Journal of Architectural and Planning Research*, 25(1): 76–90.
- Clarke, R.V. 1983. Situational Crime Prevention: Its Theoretical Basis and Practical Scope. In Tonry, M. and Morris, N. (Eds.) *Crime and Justice: A Review of Research*. Chicago, IL: University of Chicago Press.
- Countermeasures Assessment and Security Experts, Waite & Associates, and Nakanishi Research and Consulting. 2007. *Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers* (TCRP Report 86). Washington DC: Transportation Research Board.
- Crowe, T.D. 1991. *Crime Prevention through Environmental Design and Space Management Concepts*. London: Butterworth-Heinemann.
- Federal Bureau of Investigation. 1999. *Terrorism in the United States, 1999*. Washington, DC: Federal Bureau of Investigation.
- Federal Emergency Management Agency. 2003. *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*. Washington, DC: FEMA.
- Federal Transit Administration. 2004. Transit Security Design Considerations, Appendix A: Chronology of Terrorist Attacks Against Public Transit. Washington, DC: US Department of Transportation. Available at <http://transit-safety.volpe.dot.gov/security/securityinitiatives/designconsiderations/CD/appa.htm>. (accessed on March 2, 2015).
- Felson, M.E.A. 1996. Redesigning Hell: Preventing Crime and Disorder at the Port Authority Bus Terminal. In Clarke, R.V. (Ed.) *Preventing Mass Transit Crime*. Monsey, NY: Criminal Justice Press.
- Fink, C., Taylor, B., and Loukaitou-Sideris, A. 2005. From Policy and Response to System Design and Operations: Trends in Inter-Governmental Transit Security Planning in the U.S. *Journal of Public Transportation*, 8(4): 1–16.
- Fries, R., Chowdhury, M., and Brummond, J. 2009. *Transportation Infrastructure Security: Utilizing Intelligent Transportation Systems*. Hoboken, NJ: John Wiley & Sons, Inc.
- Goetz, E. 2003. On The Road to Transportation Security. Hanover, NH: Institute for Security Technology Studies Dartmouth College. Available at: <http://www.ists.dartmouth.edu/library/217.pdf> (accessed on March 1, 2015).
- Harris, O. 1971. *A Methodology for Developing Security Design Criteria for Subway*. Washington, DC: Urban Mass Transit Administration. Report No: UMTA-URT-5 (70)-71-4.
- Hartgen, D., Ingalls, G., and Owens, T. 1993. *Public Fear of Crime and its Role in Public Transit Use*. Raleigh, NC: University of North Carolina, Center for Interdisciplinary Transportation Studies.
- International Association of Public Transport (UITP). 2009. PT9, Anti-Terrorism Public Awareness Campaigns, COUNTERACT Final Report.
- International Association of Public Transport (UITP). 2010. Secure Public Transport in a Changeable World. Available at [http://www UITP.org/sites/default/files/cck-focus-papers-files/focus\\_security\\_en\\_OK.pdf](http://www UITP.org/sites/default/files/cck-focus-papers-files/focus_security_en_OK.pdf) (accessed on April 7, 2015).
- Jacobs, J. 1961. *The Death and Life of Great American Cities*. New York: Vintage Books.
- Jenkins, B.M. 2001. *Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview*. Report FHWA/CA/OR 2001–29. San Jose, CA: Norman Y. Mineta International Institute for Surface Transportation Policy Studies.

- Jenkins, B.M. and Butterworth, B.R. 2007. *Selective Screening of Rail Passengers*. Report 06-07. San Jose, CA: Norman Y. Mineta International Institute for Surface Transportation Policy Studies.
- Jenkins, B.M. and Butterworth, B.R. 2010. *Explosives and Incendiaries Used in Terrorist Attacks on Public Surface Transportation: A Preliminary Analysis*. Report WP 09-02. San Jose, CA: Norman Y. Mineta International Institute for Surface Transportation Policy Studies.
- Jenkins, B.M. and Gersten, L. 1997. *Protecting Surface Transportation Systems and Patrons from Terrorist Activities: Case Studies of Best Security Practices and a Chronology of Attacks*. San Jose, CA: Norman Y. Mineta International Institute for Surface Transportation Policy Studies.
- Jenkins, B.M. and Trella, J. 2012. *Carnage Interrupted: An Analysis of Fifteen Terrorist Plots Against Public Surface Transportation*. Report 11-20. San Jose, CA: Norman Y. Mineta International Institute for Surface Transportation Policy Studies.
- LaFree, G., Dugan, L., and Miller, E. 2012. *Integrated United States Security Database (I USSD): Data on the Terrorist Attacks in the United States Homeland, 1970 to 2011. Final Report to the Resilient Systems Division, DHS Science and Technology Directorate*. College Park, MD: U.S. Department of Homeland Security National Consortium for the Study of Terrorism and Responses to Terrorism.
- LaVigne, N.G. 1996. Safe Transport: Security by Design on the Washington Metro. In Clarke, R.V. (Ed.) *Preventing Mass Transit Crime*. Monsey, NY: Criminal Justice Press.
- Loukaitou-Sideris, A. 2012. Safe on the Move: The Importance of the Built Environment. In Ceccato, V. (Ed.) *Urban Fabric of Crime and Fear*. Berlin, New York, and London: Springer.
- Loukaitou-Sideris, A., Taylor, B., and Fink, C. 2006. Rail Transit Security in an International Context: Lessons from Four Cities. *Urban Affairs Review*, 41(6): 727–748.
- Lynch, G. and Atkins, S. 1998. The Influence of Personal Security Fears on Women's Travel Patterns. *Transportation*, 15: 255–277.
- Maag, C. 2012. WP38, Training and Simulation. SECUR-ED (Secured Urban Transportation-European Demonstration), SP3/SP4/SP5 Joint Meeting Presentation, Brussels, Belgium, June 9.
- Morgan, D. and Abramson, H.N. 2000. Improving Surface Transportation Security Through Research and Development. *TR News*: pp. 28–30.
- Myhre, M.L. and Rosso, F. 1996. Designing for Security in Meteor: A Projected New Metro Line in Paris. In Clarke, R.V. (Ed.) *Preventing Mass Transit Crime*. Monsey, NY: Criminal Justice Press.
- Newman, O. 1972. *Defensible Space: Crime Prevention through Urban Design*. New York: MacMillan Co.
- Rabkin, M., Brodesky, R., Ford, F., Haines, M., Karp, J., Lovejoy, K., Regan, T., Sharpe, L., and Zirker, M. 2004. *Transit Security Design Considerations*. Washington, DC: US Department of Transportation.
- Radatti, P. 2008. Computer and Transportation Systems Security. In Bragdon, C. (Ed.) *Transportation Security*. Burlington, MA: Butterworth-Heinemann.
- Rohlich, N., Haas, P.J., and Edwards, F.L. 2010. *Exploring the Effectiveness of Transit Security Awareness Campaigns in the San Francisco Bay Area*. San Jose, CA: Mineta Transportation Institute, College of Business, San José State University, 72pp.
- Rothman, P. 2012. STE Security Innovation Awards Silver Medal: Technology Makeover. *Security Info Watch*, December 10, 2012. American Public Transportation Association.

- Schulz, D. and Gilbert S. 2011. Video Surveillance Uses by Rail Transit Agencies. In *Transportation Cooperative Research Program Synthesis 90*. Washington, DC: Transportation Research Board. Available at: [http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp\\_syn\\_90.pdf](http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_syn_90.pdf) (accessed on March 1, 2015).
- SECUR-ED SP3/SP4/SP5 Joint Meeting Presentation. 2012. WP38 ‘Training and simulation,’ Brussels, June 9, 2012, Christian Maag, University of Wuerzburg, Wuerzburg.
- Taylor, B., Loukaitou-Sideris, A., Liggett, R., Fink, C., Wachs, M., Cavanagh, E., Cherry, C., and Haas, P. 2005. *Designing and Operating Safe and Secure Transit Systems: Assessing Current Practices in the United States and Abroad*. San Jose, CA: Mineta Transportation Institute.
- Transit Cooperative Research Program. 2007. Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers. In *TCRP Report 86 – Public Transportation Security, Volume 13*. Washington, DC: Transportation Research Board.
- UITP. 2009. PT9—Anti Terrorism Public Awareness Campaigns, COUNTERACT Final Report.
- United States Department of Homeland Security, Transportation Security Administration. A chronology and categorization of these attacks. Available at: <http://transit-safety.volpe.dot.gov/security/securityinitiatives/designconsiderations/CD/appa.htm>. (accessed on March 2, 2015).
- United States General Accounting Office. 2002. Mass Transit: Challenges in Securing Transit Systems. In *Testimony Before the Subcommittee on Housing and Transportation. Committee on Banking, Housing and Urban Affairs, U.S. Senate*. Washington, DC.
- Wilson, J.Q. and Kelling, G.L. 1982. Broken Windows: The Police and Neighborhood Safety. *Atlantic Monthly*, 249(3), 29–38.
- Yellow Design Foundation. 2008. *Spin Up: Design and Human Engineering of Urban Public Transport, Brussels, Belgium*. Available at: [http://www.ydesignfoundation.org/img/PDF/SPIN-UP\\_EN\\_AUGUST2013.pdf](http://www.ydesignfoundation.org/img/PDF/SPIN-UP_EN_AUGUST2013.pdf) (accessed on March 2, 2015).

### **People Interviewed in the Course of Preparing This Chapter Who are Cited as Sources of Information**

- Richard Gerhart, Security Team Leader, Federal Transit Administration, interview by Camille Fink, November 6, 2012, Washington, DC (telephone).
- Gregory Hull, Director—Operations, Safety and Security Programs, American Public Transportation Association (APTA), interview by Camille Fink, October 26, 2012, Washington, DC (telephone).
- Lindsey Mancini, Regional Officer, North America, International Association of Public Transport (UITP), interview by Camille Fink, November 22, 2012, Brussels, Belgium (email).



---

# 9

---

## RAILROAD INFRASTRUCTURE: PROTECTING AN INCREASINGLY VULNERABLE ASSET

JEREMY F. PLANT<sup>1</sup> AND RICHARD R. YOUNG<sup>2</sup>

<sup>1</sup>*Department of Public Policy and Administration, Penn State Harrisburg—The Capital College, Pennsylvania State University, Middletown, PA, USA*

<sup>2</sup>*School of Business Administration, Penn State Harrisburg—The Capital College, Pennsylvania State University, Middletown, PA, USA*

### 9.1 INTRODUCTION

In the summer of 2013, a series of catastrophic accidents involving trains has drawn attention to the risks and vulnerabilities inherent in this mode of transport. The small community of Lac-Mégantic, Quebec, was devastated by explosions and fires from the derailment at high speed of a runaway oil train, with 47 people killed and much of the town destroyed. A passenger train in northwest Spain derailed at over twice the speed limit, witnessed by thousands in a chilling YouTube video of images captured by a surveillance camera; the death toll at the time of this writing was 79 and expected to rise. Even the Swiss rail system, considered one of the safest in the world, experienced a fatal head-on collision at Granges-pres-Marnand, near Bern, on July 30, killing the engineer of a fast-moving passenger train.

Although all three of these tragic incidents seem to have their cause in human error, they expose a major reality: even though statistically rail is at or near the top of the list of safest modes of transport, there are real risks inherent in rail operations, and the consequences of rail mishaps, whatever their cause, have the potential to be

catastrophic. Compared to the extensive levels of security employed in air transport, rail is a “soft target” to terrorists and by its nature is difficult to secure. Added to the inherent problems of securing the vast rail network is the public perception that rail security is of secondary concern compared to other modes. Although popular opinion in the United States has often relegated railroads to the trash bin of history, this chapter aims to educate the reader to the growing importance of this mode and the need to craft procedures and policies to ensure the security of the far-flung rail network.

The security of railroads has never been more important than in the post-9/11 era. For the past 30 years, railroads in the United States have experienced an unprecedented growth in volume—both freight and passenger rail operations are seeing major increases in nearly every geographic market. Passenger traffic on many intercity routes and all major commuter corridors is on the rise; freight traffic up until the Great Recession has been at record levels; new markets, most notably in recent years domestic petroleum movements, are being developed; and investment in freight rail is seeing its third straight record year, with over \$14 billion allocated for new capital spending on infrastructure improvement projects and rolling stock for calendar 2013 (Morris 2013)—a dramatic turnaround given that the railroads were seen by many as a dying industry in the 1960s and 1970s with some pundits all but writing their obituaries.

Despite these trends, which for the most part began back in the early 1980s, rail has often been an underdeveloped element in planning for critical infrastructure protection. Although worldwide passenger rail has been a frequent target for terrorists since as early as the late 1800s and especially in the past 10 years, there have been no catastrophic events in the United States to galvanize interest in rail security the way there has been for air transport. The movement or storage of hazardous materials in urban areas has raised public attention somewhat to threats to freight movements, but the full range of vulnerabilities and threats is largely unknown to the public at large. The Transportation Security Administration (TSA) of the Department of Homeland Security (DHS) has responsibility for rail security, but has focused the bulk of its attention as well as resources to airline security with the result that the railroad companies themselves have assumed many of the responsibilities for ensuring security from both terrorist events and natural calamities alike.

Nevertheless, there are positive signs along with that lurking sense of vulnerability. Perhaps with the exception of the derailing of Amtrak’s *Sunset Limited*, presumably by domestic terrorists, in the Arizona desert in 1995, the United States has not experienced the attacks on passenger trains as seen in other parts of the world, notably Western Europe, Russia, and India. These attacks have led to substantial casualties: 52 civilians and four bombers killed and 700 injured in the July 7, 2005, London bombings; 191 dead and over 1800 wounded in the March 11, 2004, Madrid commuter train attacks; 25 killed in the bombing of the Nevsky Express in Russia in November 2009; and 209 killed and 700 injured in the attack of Mumbai commuters on July 11, 2006. Moreover, there have been more recent noteworthy attempts such as the thwarting of a terrorist plot in Canada in early 2013; however, due to early detection, the threat was averted, and there were no injuries or loss of life.

Second, the rail industry has fostered extensive cooperation with government at all levels since September 11, 2001, to develop an integrated system of intelligence, information sharing, and planning. Third, the railroads are differentiated from other transport modes with their long-standing establishment of a highly skilled and professional corps of police officers trained at railroad-owned and railroad-operated police academies recognized by civil authorities for their quality and capabilities. Fourth, the rail industry has the ability to marshal considerable resources to quickly recover from catastrophic damage to its infrastructure. A good example was the resumption of service across Lake Pontchartrain in the wake of Hurricane Katrina in 2005. Norfolk Southern's line across the 5.8 mile bridge over Lake Pontchartrain was severely damaged, with over five miles of track washed into the lake. A concentrated effort to rebuild the bridge and nine miles of NS tracks in the city of New Orleans damaged in the storm resulted in the opening of the line after only 16 days.

In this chapter, we review the nature of vulnerabilities and threats to the rail system in the United States, identify the policy approaches to ensuring rail security, and place the rail system in the context of the American economy and society. A key factor that we consider is the continuing development of information sharing and methodologies to assess threats and vulnerabilities and the development of recovery and resilience models for potential catastrophic events. Also considered are ways in which scenarios are or can be developed to deal with likely threats and vulnerabilities, such as weapons of mass destruction conveyed on intermodal freight trains or bombings of crowded commuter trains, stations, and rights-of-way. It raises a serious question: if rail is a relatively soft target, what measures have been taken to ensure security, and what remains to be done?

The chapter concludes with a series of recommendations based on five recurring themes that underscore the need for a strategic approach to rail security: the importance of rail transport in the economy and society, the interconnectivity of railroads with other modes of transportation and critical sectors of the economy, the ongoing need to maintain an effective program of *rail safety* but to also differentiate this from the topic of *rail security*, the need to develop an understanding of the risks and vulnerabilities of both freight and passenger rail operations as interconnected entities within a common network, and the need to develop reliable measures of risk when relevant empirical data is not available.

## 9.2 RAIL VULNERABILITIES AND THREATS

The US rail system is an interconnected complex network consisting of more than 190,000 miles of standard gauge track; operated by more than 550 separate companies, government agencies, and quasigovernmental authorities; located in 49 US states; and running over both desolate and urban terrain where more than 100,000 key structures such as bridges, culverts, and tunnels (Harrison 2007). While the United States has some narrow gauge operators, these do not operate in interchange with the rest of the system and their total mileage is negligible. Of the approximately 550 operators, there are a single national passenger railroad, Amtrak; 18 noteworthy commuter

railroads; seven Class I major freight railroads; and hundreds of short lines (regional, local, terminal, and switching railroads with routes ranging in length from under one mile to several hundred miles). The United States increasingly has light rail passenger systems whether they are elevated, subterranean, or surface types, but these, too, do not operate in interchange with the national network. In the aggregate, US railroads operate more than 25,000 locomotives, 400,000 freight cars, and thousands pieces of passenger equipment. The volume of annual moves is significant to the US economy with the system handling over 30 million carloads, 12 million intermodal moves, and eight billion passenger trips annually (American Association of Railroads 2013).

By definition, the network includes several other major participants, including the private owners and/or operators of freight cars of which there are more than 700,000 (Official Railway Equipment Register 2011) and those firms known as intermodal service providers such as truckers (e.g., United Parcel, J.B. Hunt, and Schneider National) or intermodal retailers (e.g., Pacer Stacktrain, Alliance Shippers, and the Hub Group). Intermodal equipment interchange terminals, necessary for loading and unloading from the rails, have their own perhaps unique security issues.

While much of the discussion of rail security focuses on human-caused threats to the railroad network, most notably terrorist activity, the nation still must remain vigilant to protecting it from an extensive range of natural threats. Securing the rail system requires that attention be given to all types of threats as well as an examination of those mechanisms whereby they may be anticipated, defended against, minimized, and remediated. Consider, for example, Table 9.1 that provides a basic taxonomy of these, each element of which shall be subsequently discussed.

Note that the natural threats to railroads are common for both passenger and freight systems; these may often affect both freight and passenger systems concurrently because both modes often share common rights-of-way. A primary example is the heavily trafficked Northeast Corridor, owned by Amtrak but also used by several commuter railroads, Class I freight railroads, and freight short lines. The opposite is true of the CSX-owned right-of-way across northern New York State where Amtrak and several short lines can be found as tenants with trackage rights (Kalmbach 2010).

**TABLE 9.1 Classification of Threats to Railroads**

	Human-Caused Unique Events	Human-Caused Common Events	Natural Events
Passenger	Terrorist acts against passengers	Terrorist acts against rail infrastructure	Flooding
	Theft of passenger property	Damage to railroad property	Hurricanes
Freight	Theft of freight	Theft of railroad property	Wind
	Damage or tampering with freight	Injury or death to persons or property adjacent to railroad	Wildfire
		Accidents	Tornados
			Blizzards
			Ice storms
			Excessive heat

*Source:* Plant et al. (2013).

Shared rights-of-way are also a consideration when considering human-caused threats where the objective may be damage to freight infrastructure by targeting passenger equipment or vice versa.

Intermodal transportation is solely in the freight sector. Either ocean containers or highway trailers are taken off the roads and transported long distances by the railroads. As such, intermodalism has unique vulnerabilities and threats that potentially include (i) long chains of multiple possession, shippers, truckers, container terminals, ocean carriers, intermodal terminals, and railroads; (ii) chains of possession that are often outside of the United States; (iii) contents that often are of higher value than usual rail-borne freight (much rail freight continues to be bulk materials including coal and ore, sand and aggregates, fertilizer, chemicals and plastics, grain, and petroleum, whereas containers will carry processed food, electronics, industrial equipment and its components, and textiles including clothing); and (iv) contents that are not known to the railroad other than, for example, “one 40’ container.”

Historically, most threats to rail networks have targeted passenger trains, with such notable recent examples as the aforementioned Madrid commuter train bombings, numerous incidents in India, and at least one in Russia. Freight railroads can be targets because of the proportion of economic activity that they represent, but also in an era where many firms are practicing just-in-time inventory strategies, any disruption risks shutting down entire firms and even vertically chained industries.

In addition to human-caused actions, railroads are particularly vulnerable to natural events because (i) the nature of their infrastructure is often found in desolate locations far from civilization and any security presence; (ii) much of their infrastructure traverses high-crime urban areas; (iii) some freight, especially containerized, is high value, thus with high theft appeal; (iv) some freight is classified dangerous including, but not limited to, poisons, flammables, oxidizers, and corrosives—chlorine, propane, ethylene oxide, and alcohols—(v) these have lines with very high volume of activity and some with nearly nonexistent traffic; (vi) and these are private corporations that while having their own police forces, these are very small and their cooperation with law enforcement is inconsistent. It is this last point that will receive much emphasis in a later section of this chapter called *connections*.

Rail networks are susceptible to natural disasters, and in recent times, there have been instances of rights-of-way damaged by the likes of Hurricane Katrina on the Gulf Coast and Hurricane Sandy in the Northeast, but flooding in the Midwest and blizzards in various parts of the country still inflict damage to infrastructure that has immediate economic consequences for the affected railroads. Moreover, there is an economic impact on the shippers and consignees of the freight as well as the passengers involved.

### 9.3 SECURING RAIL OPERATIONS

The Aviation and Transportation Security Act (2001) created the TSA. TSA, originally a part of the Department of Transportation (DOT), was intended to be the one federal agency responsible for the security of all modes of transportation. The DHS, created in 2002, acquired TSA on March 1, 2003 (Homeland Security Act 2001).

Upon its establishment, TSA focused primarily on aviation security largely ignoring the other modes. Most of its workforce was based at airports, and most federal security regulations and policies were aviation centric, a focus that continued even after the London and Madrid bombings.

Congress, recognizing the glaring gap in rail security, passed H. R. 1, titled *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Commission Act), in July 2007. Rail security provisions were included in Title XV, Surface Transportation Security: Subtitle B, sections 1511–1528. Summarized, the provisions included:

- Creation of a federal task force under DHS leadership and composed of representatives of appropriate federal agencies, whose charge is to complete a nationwide risk assessment of a terrorist attack on US railroads.
- Requirement that DHS develop and implement a National Strategy for Railroad Transportation Security, including a description of the responsibilities of other levels of government and additional stakeholders.
- Each major railroad is required to conduct a vulnerability assessment and present a security plan to DHS within 1 year of passage of the legislation, assisted by DHS.
- Each railroad's security plan required identification of a security coordinator to be the link with the government.
- Railroad security plans were required to be periodically updated and reviewed by DHS.
- DHS will provide grants to railroads to enhance security.
- Special attention was to be given to testing railroad tank car vulnerability.
- Funds were to be made available to Amtrak for general passenger security and key initiatives, especially the Northeast Corridor with its vulnerable tunnels.
- Funds were to be available through DHS for rail security training programs, mock terrorist attacks to test responses, and research on rail security.
- Issues of border security for both freight and passenger rail operations were to be included.

The intent of the legislation clearly was to incentivize the federal government to devote more resources and attention to rail security.

As the agency designated to oversee rail security programs, TSA employs over 45,000 people, 175 of whom are designated surface transportation security inspectors (STSI) (TSA 2013) responsible for implementing the 9/11 Commission Act recommendations and are stationed around the country. Reporting to respective airport federal security directors (FSDs), these inspectors are tasked with conducting voluntary vulnerability assessments and regulatory compliance inspections.

During recent years, Congress and industry officials have been very critical of the STSI program, especially because most have no surface transportation expertise. At the commencement of hearings in May 2012 before the House Subcommittee

on Transportation Security, Chairman Rogers noted that their leadership, the FSDs, have no such experience either. CSX executives, witnesses at the hearing, stated that their firm was “very troubled by the lack of consistency in STSIs’ interpretation of regulatory requirements and their subsequent actions especially with regard to the transport of hazardous materials” (House Homeland Security 2012). John O’Connor, chief of Amtrak Police, stated that it was unclear whether the program, as funded and structured, added value to overall security efforts (House Homeland Security 2012).

In a 2012 report, the Government Accountability Office (GAO) expressed concerns with the STSI program finding that TSA “had inconsistently overseen and enforced its rail security incident reporting requirement.” Moreover, GAO recommended that TSA develop guidance on the types of incidents that should be reported and enhance existing oversight mechanisms for compliance inspections and enforcement actions (GAO 2012a).

TSA must hire additional STSIs and revamp the current STSI program if it is to be considered a relevant part of the agency’s layered security approach. In addition to completing the GAO recommendations, TSA should ensure that its STSIs are properly trained. Current STSIs must be required to demonstrate advanced knowledge of the railroad and mass transit industries. That knowledge should come from actual experience and not be dependent upon information from either books or the Internet (GAO 2012a).

Similarly, future STSIs should be hired from the ranks of those with actual experience, and working at an airport is not the equivalent to employment in the rail industry (GAO 2012a).

Grants from the federal government are critical to the development of a comprehensive approach to rail security. TSA works with the Federal Emergency Management Agency (FEMA) to distribute grants to rail and mass transit system operators. FEMA is responsible for administering the Transit Security Grant Program (TSGP) and the Intercity Passenger Rail Grant Program (IPRGP). As such, it is responsible for ranking and rating rail and mass transit assets, nationwide. The relationship between FEMA and TSA was formalized in a memorandum of understanding in June 2011.

Working together, the two agencies have allocated \$547 million to 60 mass transit and passenger rail systems in 25 states and the District of Columbia (TSA 2012a). The money was spent on emergency preparedness drills and exercises, public awareness campaigns, and the protection of high-risk underground rail assets. The ubiquitous “see something, say something” campaign, surveillance cameras, and roving canine patrol teams are the most visible signs of the expenditure of these funds.

A problem with the grant program is that FEMA has not always allocated funding in an expeditious manner. At a July 2012 hearing of an oversight Senate Subcommittee (2012), the FEMA assistant administrator stated that staffing shortages have hindered its review process and further noted that the agency’s delays have negatively impacted the grantees ability to proceed with critical projects. As a result of the government’s delays, grantees have now been permitted to reprogram spending for more urgent needs (GAO 2012b).

The government is now endeavoring to combine the 16 current separate grant programs into a single system. In the past, transit security grants went directly to mass transit and passenger rail systems, but under the bundling concept, agencies would need to compete against nontransit agencies for homeland security funds. The American Public Transportation Association (APTA), representing the nation's mass transit systems, opposes this proposal requesting that Congress continue to appropriate money directly for public transportation. APTA's opposition stems from the fear that some state administrators may not consider the security of passenger rail systems as important as those threats to other parts of the nation's critical infrastructure (APTA 2012).

GAO has expressed its concern that the current grant distribution process may have possible overlap with the TSGP and the State Homeland Security Grant Program, the Urban Area Security Grant Program, and the Port Security Grant Program—these all have similar goal and fund similar projects. In its 2012 report, GAO stated that FEMA lacks a process for coordinating reviews across the four programs and recommended that the agency explore opportunities to enhance internal coordination and administration of the program (GAO 2012b).

It is imperative that FEMA work with mass transit and the passenger rail system to improve the grant review process. Grantees cannot expend funds until FEMA allocates it; hence, the more expeditious the process, the more secure the nation's passenger systems will be. Moreover, FEMA should not expend funds for duplicative projects and should seek to improve the effectiveness and efficiency of allocating scarce funding.

The current administration has been repeatedly criticized for its failure to share quality information with the rail and mass transit stakeholders in a timely manner. When President Obama took office, he tasked his staff with conducting a Surface Transportation Security Priority Assessment. One of its 2010 recommendations was to implement a unified environment for sharing transportation security information that provides all relevant threat information and its efficient flow among stakeholders (Surface Transportation Security Assessment 2010).

Two years later, the issue remained unresolved. Again, CSX's appearance before the Congressional committee underscored that "sluggishness and inconsistency with the sharing of important intelligence information from government hinders our ability to respond to potential threats" (House Homeland Security 2012). The problem continues as the administration still struggles to share information and the recent release of Presidential Policy Directive (PPD) 21—Critical Infrastructure Security and Resilience states that "[G]reater information sharing within the government and with the private sector can and must be done" (Presidential Policy Directive 2013).

The rail and mass transit systems are not waiting for the government to improve the information sharing process, but rather have developed their own information system, the Rail Action Network (RAN), in conjunction with the American Public Transportation and Public Information and Analysis Center (ST-ISAC). RAN now issues Transit and Rail Intelligence Awareness Daily (TRIAD) reports that are shared with rail and mass transit firms and agencies across the country and contain

information about recent suspicious activities and issues concerning general security awareness (Surface Transportation ISAC 2013).

#### **9.4 STEPS TO ENHANCE SECURITY**

Although ongoing policies and procedures have made the rail network more secure and safe than it was before 9/11/01, there are a number of steps that need to be taken to enhance security and to provide greater protection against likely threats and vulnerabilities. These include the following:

- TSA must hire additional STSIs and revamp its current STSI program if it is to be considered to a relevant part of the agency's layered security approach. In addition to completing the GAO recommendations, TSA should ensure that its STSIs are properly trained. Current STSIs must be required to demonstrate advance knowledge of the railroad and mass transit industries. The knowledge should come from actual experience and not be dependent upon learning information from a book or the Internet. Similarly, future STSIs should only be hired if they have actual experience; working at an airport is not equivalent to working in the rail industry.
- FEMA must work with mass transit and passenger rail systems to improve the grant review application process. Grantees can't spend the money until FEMA allocates it, so the faster FEMA allocates the money, the faster the money can be spent to secure our nation's passenger rail and mass transit systems. FEMA must also develop a process by which it tracks all of its grant allocations. The agency should not expend funds for duplicative projects. Eliminating duplication will save the government money and allow for the nonduplicative funding to be spent on more systems.
- The federal government should make improving information sharing a priority. Rail and mass transit systems cannot implement new security measures if they are unaware of suspicious activity that only the federal government knows about. Similarly, these same systems must receive quality information in a timely manner. Information that is outdated or not relevant cannot be acted upon properly.

#### **9.5 CONCLUSIONS**

The rail network is critical to the economic and social well-being of the nation. While this fact might have seemed questionable a generation ago when freight railroads were falling into bankruptcy to the extent that the Northeast came remarkably close to losing its rail freight service, and when private rail operators no longer found passenger operations profitable or desirable, it is clearly now both viable and more vital than it has ever been. This may be part of the current problem. Many still believe

that rail is an antiquated and therefore outmoded form of transportation. This belies the reality of the rail industry today, both its freight and passenger components. Conditions have changed dramatically since 1980 with all the major freight railroads being both solvent and profitable. Short line and regional railroads have proliferated and add to the fabric of freight railroading. Passenger demand has increased for both Amtrak and the commuter rail system operators. Moreover, the potential for high-speed rail systems has become a priority of state and federal political leaders across the country. New light rail and mass transit systems are seen in every region of the United States and have become a necessity for any urban area that wishes to see itself as a global player.

The rail network is all about connections. The system itself is a seamless and interconnected entity, comprising the three main components that share a common 4 ft 8½in. standard track gauge: intercity and commuter passenger operators, the seven Class 1 major carriers, and the over 500 short line and regional carriers. Rail is also about connections with other modes and industries: ports, truckers and draymen, and marine operators, who operate in concert to move the growing volumes of intermodal goods; shippers, who continue to operate their own rolling stock, employ crews to switch their yards, and police their operations; and logistics and information management specialists and marketers, who team with railroads to plan and manage the movement of goods from point to point.

Rail safety and rail security, while intertwined, are not synonymous. *Security* is defined as the domain of protecting material and human assets from any form of deliberate damage or destruction, while *safety* is the protection from natural and inadvertent man-made activities. The word *protection*, however, applies in both instances even if the latter is by way of a more formalized approach codified in law and industry standards (Edwards and Goodrich 2013). Conversely, security represents threats that continue to evolve over time, meaning that protection needs to evolve with them through an ongoing sharing of best practices. Infrastructure, therefore, requires protection from myriad threats and causes, whether natural or man-made.

There is a long history of policy and programs regulating the rail industry in the name of safety, many dating back to the ills of the industry in the late nineteenth and early twentieth centuries when railroads were among the most unsafe businesses in society. Programs to enhance safety are critical to maintaining the extremely high level of performance achieved by the railroads and to protect society against unnecessary danger, whether onboard trains, trackside at grade crossings, or in adjacent residential neighborhoods. But these efforts, largely entrusted to the Federal Railroad Administration of the US DOT and respective state DOTs, are not the same as efforts to secure the rail system from terrorism or other low-probability, high-impact events. Safety efforts focus on routine inspection of equipment and other elements of the continuous operations of the rail industry. They are designed to insure that the system operates safely and reliably, but put little or no emphasis on the projection of risk or the motives of those who might seek to disrupt the operation of the rail network. Preventing accidents caused by worn equipment or poor employee awareness is fundamentally different from the intelligence gathering and risk analysis-based approach of the post-9/11 world and as such has been entrusted to the TSA, working alongside the labyrinth of public and private organizations concerned with rail security.

Passenger rail and freight rail have both similarities and clear differences that must be reflected in policies and programs to secure the rail system. The differences relate to organization and ownership, mission and objectives, vulnerability to particular forms of disasters, consequences related to catastrophic events, and risk assessment and methods of analysis. The similarities are based on the sharing of much trackage and infrastructure or the close proximity of one to the other, the need to share intelligence and information on threats and risks, and the public's sense that the rail system can be considered a conjoined, single mode of transportation.

It is difficult yet critical to define and assess array of the risks to the rail system. Risk assessment is by nature conjectural and uncertain but especially so when there is little empirical evidence upon which to base the nature and probability of threats and the possible motives of those seeking to disrupt and harm the rail system either for its sensational news value or its potential adverse effects on economic well-being. Yet we know that the approaches of the past, or those used in other transportation modes, will not work in the New Normalcy. It is impossible to police, provide surveillance, and guard such a huge and diverse system if the goal is zero tolerance for catastrophic events. Not unlike many other modern organizations, the railroads are also vulnerable to cyberattack. All of the Class I freight railroads, Amtrak, the commuter lines, and many of the regional railroads have computer-based signaling and communications systems necessary for their efficient and routine safe operation. Any effort to compromise these systems has the potential of causing extensive physical damage to infrastructures, trains, personnel, passengers, and freight and would also have major economic consequences for the nation as a whole.

These five themes—the critical nature of the rail system for the health and well-being of the nation, the connectivity between the rail system and other industries and modes of transportation, the need to formulate a policy regime for security that is differentiated from the inherited initiatives of safety regulation, the need to consider both the similarities and differences between passenger and freight rail operations, and the difficulty of developing a reliable system of risk assessment that goes beyond traditional means of policing and surveillance—provide the foundation on which the volume is built. The approach taken mirrors the approach we hold up as the only workable model for rail security in the New Normalcy: a partnership between the public and private sectors, with a shared goal of protecting and securing the rail system through sharing of intelligence and information. Whether or not catastrophic events disrupt rail operations, the only workable approach to ensure rail security is partnership between government and the private sector.

## REFERENCES

- APTA. (2012). Senate Appropriations Subcommittee on Homeland Security Hearing, April 30, 2012, [http://www.apta.com/gap/testimony/2012/Documents/120430\\_SenateTestimony.pdf](http://www.apta.com/gap/testimony/2012/Documents/120430_SenateTestimony.pdf). Accessed March 2, 2015.
- Association of American Railroads (2013). *Class 1 Railroad Statistics*. Washington, DC: Policy and Economics Department.

- Aviation and Transportation Security Administration Act. (2001). Aviation and Transportation Security Administration Act of 2001. Public Law 107-71. <http://www.gpo.gov/fdsys/pkg/PLAW-107publ71/html/PLAW-107publ71.htm>. Accessed March 2, 2015.
- Connor Testimony. (2012). House Homeland Security Committee, Subcommittee on Transportation Security hearing, May 31, 2012, [http://homeland.house.gov/sites/homeland.house.gov/files/Testimony\\_O'Connor.pdf](http://homeland.house.gov/sites/homeland.house.gov/files/Testimony_O'Connor.pdf). Accessed March 2, 2015.
- Edwards, E. & Goodrich, D. (2013). *Introduction to Transportation Security*. Boca Raton: CRC Press. pp. 5–6.
- Harrison, B. D. (2007). Standard Gauge. Research paper. [www.strategicstandards.com/files/Metrics.pdf](http://www.strategicstandards.com/files/Metrics.pdf). Accessed March 1, 2015.
- Homeland Security Act. (2001). Public Law 107-296, <http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/html/PLAW-107publ296.htm>. Accessed March 2, 2015.
- Kalmbach. (2010). *Kalmbach Atlas of North American Railroads*. Milwaukee, WI: Kalmbach Publishing.
- Morris, B. (2013). Boom Times on the Track: Rail Capacity, Spending Soar. *The Wall Street Journal* 27, A1.
- Plant, J., Krepp, D. & Young, R. (2013). Protecting Critical Railroad Infrastructure. Proceedings of the Infrastructure Security Partnership, Annual Meeting, U.S. Military Academy, West Point, NY.
- Presidential Policy Directive. (2013). Critical Infrastructure Protection and Resilience, February 12, 2013, <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>. Accessed March 2, 2015.
- Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security. (2012). Assessing Grants Management Practices at Federal Agencies, July 25, 2012, <http://www.dhs.gov/news/2012/07/25/written-testimony-fema-senate-committee-homeland-security-and-governmental-affairs/>. Accessed March 2, 2015.
- Surface Transportation Security Priority Assessment. (2010). [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/STSA.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/STSA.pdf). Accessed March 2, 2015.
- Official Railway Equipment Register. (2011). *The Official Railway Equipment Register*, vol. 126. Princeton, NJ: UBM Global Trade.
- Transit and Rail Intelligence Awareness Daily Report. (2013). Surface Transportation and Public Transportation Information Sharing and Analysis Center. <https://www.surfacetransportationisac.org/>. Accessed March 31, 2013.
- U.S. Transportation Security Administration. (2013). Security Programs and Initiatives. <http://www.tsa.gov/stakeholders/programs-and-initiatives>. Accessed March 2, 2015.
- U.S. Government Accountability Office. (2012a). Passenger Rail Security—Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives, GAO-13-20, December 19, 2012, <http://www.gao.gov/assets/660/650995.pdf>. Accessed March 2, 2015.
- U.S. Government Accountability Office. (2012b). Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue, GAO-342-SP, <http://www.gao.gov/assets/590/588818.pdf>. Accessed March 2, 2015.

---

# 10

---

## FREIGHT RAILROAD SECURITY: A CASE STUDY OF POST-9/11 EFFECTIVENESS

ROLAND D. PANDOLFI, JR.

*Union Institute & University, North Miami Beach, FL, USA*

### 10.1 INTRODUCTION

Recognized as being instrumental to the growth of both the United States and the world economies, the American freight railroad system's success has made the system a high-profile target for terrorists. The size of freight railroading, the global economy, and the success of the supply chain increases the possibility for a substantial attack (Flynn 2004).

An attack on one sector of the supply chain can cause a ripple effect that will negatively impact other sectors far away from the original incident (Stevens 2004). This vulnerability increased post-9/11 when US enemies concentrated on civilian targets with the goal of causing great destruction to the American homeland (Flynn 2004). Both globalization and a much more connected world have provided America with an opportunity to gain more power and more dominance in every corner of the globe. US enemies have demonstrated a propensity to use violence to avert any further American advancement, seeking to set the United States back many years (Karpov et al. 2003).

The supply chain is pivotal to the international success of economic growth and ever-increasing pressure for upward mobility that has shadowed globalization in recent years. By striking the American freight railroad system, terrorists have the

ability to impede the network that connects so many countries and markets throughout the world, including both those in the east and the west (Szylowicz 2004).

At home, even the greater part of power production is dependent on the supply chain as a very large percentage of coal is transported by freight rail carriers before the coal is taken to its destination to generate electricity (D'Amico 2006b; Plant and Young 2007).

Equally important is the reliance of the food chain on freight railroading (Flynn 2004). Foot-and-mouth disease, if introduced into the food chain, can easily cost the US economy millions of dollars. More importantly, the American public would lose complete confidence in the ability of America to deliver food to their tables (Plant and Young 2007). When foot-and-mouth disease spread in 2001, unrelated to terrorism, 10 million cattle had to be destroyed (Vlahos 2008), and the United Kingdom stopped all beef exports from America for a period of time (Flynn 2004). Therefore, it is important that food products remain safe and secure while in the custody of railroads.

Deregulation and the North American Free Trade Agreement (NAFTA) have had the largest positive influence on the freight railroad industry in modern times (Daniels 2000). As a consequence of the Staggers Act, which deregulated railroads in 1980, freight traffic has continued to improve, achieving extraordinary results (Daniels 2000). In 1994, US rail carriers significantly grew as a result of NAFTA opening up trade between Canada, Mexico, and the United States. North and south traffic was vital to this drastically increased level of business from which freight railroad carriers continue to benefit even today (Barrett et al. 2007).

The earliest documented attempt to attack the US railroad system occurred on June 13, 1943. A German submarine transported eight foreign agents to the US shore with the intention of blowing up the Limeville Bridge on the Chesapeake and Ohio Railway in Amagansett, Long Island (Plant 2004; Plant and Young 2007; Zengerle 2001). Authorities were successful in arresting the German spies involved before they could successfully carry out the attack (Zengerle 2001).

While many documented attacks have occurred against passenger rail, clearly the attacks provide beneficial insight into the capabilities of terrorists and their potential to carry out an assault on the American freight railroad system (Capra 2006). The world was overcome with disbelief by 9/11 due to the unconventional tactics that were used, changing the American homeland forever (Griset and Mahan 2003). One recent example of what can take place involving freight railroading occurred on July 2, 2010, in Dagestan, Russia. A large explosion derailed eight railcars transporting construction materials (Guterman 2010).

If the freight train contained toxic-by-inhalation chemicals, the impact would have covered a much larger geographical area and may have killed thousands. While not caused by terrorism, several accidents in the United States involving freight trains have demonstrated the intensity of hazardous chemicals when they are released into the environment (Sullivant 2007).

One person was killed, 300 injured, and more than 15,000 evacuated when a freight train hauling ammonia in the development of Terracita Vallejo, in North Dakota, was involved in an accident in June 2002 (Sullivant 2007). Seven cars

derailed and the ammonia that was released created a plume that extended over an 11-square mile area, causing this widespread catastrophic incident.

Another demonstration of the potential for widespread tragedy took place in June 2004. Two freight trains struck each other, causing the release of chlorine gas and ammonium just outside San Antonio, Texas. In addition to a railroad employee who died on the scene, two women were found deceased a mile away. Investigators believe this was the result of the plume. Another 50 people in this area experienced respiratory ailments and received medical treatment (Sullivan 2007).

In June 2009, an Italian freight train transporting liquefied gas exploded killing 22 and injuring many, including children (Associated Press 2009). This derailment was the result of a company with dated equipment and a poor safety record. A wheel axis with a fracture was a major factor in this disaster (David and Rizzo 2009). Another instance showing the vulnerability of the system occurred in March 2009 when a 120-ton locomotive was taken for a joyride in South Florida (Samuels, 2009). If the perpetrator's motive was terrorism, the outcome could have been catastrophic. This locomotive was unsupervised when this theft took place. This incident again demonstrates the vulnerability of en route security, that involving moving trains, if a terrorist attacked a train transporting highly hazardous materials.

It is an arduous task to secure the American freight railroad system due to a vast number of decentralized infrastructure that are spread over thousands of miles. Because of the difficulty in controlling access and keeping trespassers away, the track, switches, rail yards, tunnels, bridges, and buildings are susceptible to a terrorist attack (Plant 2004). Over these rails, vulnerable railcars carry hazardous materials, food, and freight from every corner of the world (Plant and Young 2007). Very few physical barriers are available to thwart terrorists from placing a bomb or deploying an unconventional attack against a freight train in transit (Szyliowicz 2004).

Moreover, the potential of a sophisticated cyberattack against the computer platforms that operate the railroads is becoming more likely. In 2011, the Bay Area Rapid Transit (BART) experienced two different electronic security breaches in protest to a shooting that occurred involving a transit police officer (Sneider 2012). While the hackers were unable to interfere with any network operating systems, threats such as these remain a clear and present danger against the American freight railroad system (Plant and Young 2007).

The largest segment of American railroads consists of seven Class I railroads that have over 140,000 miles of track and boast \$60 billion in revenues. This segment does not include an additional 21 regional and 510 local railroads. According to the Federal Railroad Administration (U.S. Department of Transportation n.d.a), the system will continue to rapidly expand between 2010 and 2035. This estimate is based on 22% cargo tonnage that is expected to increase. Moreover, by 2050, as the US population grows to an estimated 420 million citizens, the American freight railroad system will continue to grow, transporting a formidable 35% of tonnage annually.

This study investigated (i) what methods could be used by terrorists to attack the American freight railroad system, (ii) what improvements were made by stakeholders and the federal government to advance security in this new environment, and, finally,

(iii) identifying what steps can be taken to reduce the vulnerability of a violent attack against the system through target hardening.

## 10.2 RESEARCH METHOD

Direct observations of railroad infrastructure and freight trains, inspections of physical artifacts, and a broad review of legislation were collected using a holistic method for data gathering. A holistic approach is used in research when the study is broad and encompasses many different segments that must all work together proficiently. The decision to use a holistic method for data gathering was twofold. First, a holistic approach works hand in hand with the systems theory, particularly when studying the behavior of large complex systems, such as railroading. Many organizations and stakeholders are involved in shoring up railroad security (Patton 2002). Second, a holistic approach is beneficial in gaining a 360-degree perspective that is necessary to understand how the many working entities in the entire system communicate with each other to improve security management (Jordan and Reed 2007; Patton 2002). Selecting an alternative data-gathering method could have exposed this project to the possibility of omitting essential evidence. Qualitative in nature, the goal was to assess all data and describe themes, interpretations, and assertions.

The holistic approach was centered on von Bertalanffy's (1968) general systems theory. The general systems theory was selected because it provides a framework to examine how the many different entities and stakeholders work together in attaining the ultimate goal of making the US freight railroad system more secure. Moreover, the approach helps to identify potential gaps between these many partners and their responsibility and scope of authority. In order to understand one part or section within the system, the data often must demonstrate the interaction between two or more parts within the entire body of research. In the case of freight rail security, many parts thereof must work in sync with each other to be effective.

The research population for this study included the many stakeholders responsible for securing the American freight railroad system. The population encompassed, in part, the carriers themselves, the Transportation Security Administration, the U.S. Department of Homeland Security, the Federal Railroad Administration, the Association of American Railroads, the law enforcement community, and any law-making entity with lawful authority to enact legislation that would improve freight railroad security in the United States.

A nonrandom sampling frame was used for this case study. The American freight railroad system was the sampling frame. The reason that a nonrandom sampling frame was selected was due to convenience. Because of the significant size of the entire system and the fact that both railroads selected operate in urban and rural areas and travel through large and small cities would have no influence on the results. The reason that differentiation is made between urban and rural areas is because the risk for collateral damage is higher in an urban area. Moreover, the railroad system is so large that it would not be practical to study beyond a specified geographical scope as was done in this case.

The two freight railroads that were chosen for this case study encompassed less than 1% of the sampling frame. These railroads were selected because of their accessibility to the railroad-owned private property. The private property was where the direct observations and the inspection of physical artifacts took place. This subgroup of the American freight railroad system possessed equivalent characteristics as any other carriers throughout the United States. Due to the sensitivity of the case study, the railroads allowed the investigator access to the property under the condition that their names would not be disclosed. Therefore, hereafter, the railroads are referred to as Railroad A and Railroad B. Railroad A is a Class I major (U.S. Department of Transportation n.d.b) carrier that traverses 20,000 miles of track, whereas Railroad B is a Class II (U.S. Department of Transportation n.d.c) regional carrier that traverses 350 miles of track.

Two phases of direct observation were conducted in order to inspect and to gather data relevant to Railroad A and Railroad B. To complete the first phase, the investigator participated in a ride-along with law enforcement officers from Railroad A and from Railroad B. During each ride-along, the investigator used this opportunity to inspect the railroad infrastructure and the property. In the second phase, the investigator conducted inspections of the railroad infrastructure and the property without any supervision from railroad officials. This was done without trespassing on carrier property; therefore, certain portions of the access were limited. All data gathered were organized into a case study database.

A case study database was created to catalog and organize the evidence that was gathered by the investigator throughout the project. By having a mechanism in place, such as a case study database to maintain and manage the evidence, the reliability of the case study was improved (Yin 2003). As the direct observations and the literature review produced data for collection, the data were accurately detailed in field notes. Once the investigator returned to the office, the field notes were used to enter the evidence into the database so that it could be organized and methodically examined to establish if the evidence was appropriate for responding to the research inquiries. The investigator also made sure that a causal link was existent. If a case study database was not employed, the integrity of the research project may have been jeopardized by including data that truly did not pertain to the intended research (Yin 2003).

## 10.3 FINDINGS

### 10.3.1 Direct Observations

The investigator observed trespassers on the property of both carriers. Trespassing is evidently a significant problem that creates a void in protecting railroad infrastructure from terrorist threats. Additionally, substantial quantities of criminal graffiti were observed on many railcars, engines, buildings, and bridges. Railroad police agents conducted very proactive enforcement by stopping, challenging, identifying, and warning many trespassers. Nonetheless, a culture persists where individuals feel as if they can come and go, trespassing throughout the carrier's right-of-way, without

any level of culpability. The overall number of agents is nominal compared with the hundreds and thousands of miles of unprotected carrier property.

The investigator was able to inspect a major rail yard for each of the carriers. A considerable difference was observed between Railroad A and Railroad B. Both rail yards were located in a major US metropolitan city where high crime rates prevail. Railroad A's yard was susceptible to terrorism threats due to several weaknesses in security that were observed. The ability for trespassers to enter and commit acts of terrorism or crime was high due to various points of entry with limited or no access control. Even if visitors obtained valid ID badges to enter, there was little or no supervision, allowing the visitors to roam freely throughout the property. It should be noted that Railroad A's rail yard was also used by two other passenger carriers.

Railroad B's yard also encompassed a major intermodal facility. Security management was incomparable for several reasons. First, the yard was physically secured by fences, secured gates, and natural barriers. Second, all access was managed by either civilian security or sworn law enforcement agents, face-to-face or via remote technology. Third, all visitors were vetted, monitored, and required to wear visible issued credentials. Fourth, the fueling stations, intermodal depot, and tank cars were protected and treated as high-level targets that were more vulnerable to being breached than other sections of the property.

Trespassers were observed fishing contiguous to a bridge owned by Railroad A. The trespassers were quickly challenged, interviewed, and warned by the railroad police agents. Railroad A's agents stated that critical infrastructure, such as bridges, have alarms, sensors, voice-over technology, and surveillance cameras. Under certain circumstances, the dispatcher located in the command center can warn trespassers via voice-over technology to leave the property. Railroad A's agents randomly perform inspections via boat under many of the bridges, looking for suspicious activity, contraband, and, particularly, explosives. The investigator did not identify any use of alarms, sensors, voice-over technology, or surveillance cameras along the main line of Railroad B. This does not necessarily mean that they do not employ such technology somewhere in the system. Furthermore, Railroad B does not have any mechanism in place to inspect underneath any of the bridges on its right-of-way.

Rail switches owned by both carriers were unprotected, and both railroads had unattended engines and railcars scattered throughout the main line and sidings. En route security was similar due to the nature of railroading and the absence of quantifiable barriers. The inability to insulate engines and railcars in transit is a visible security weakness that increases vulnerability to terrorism. The substantial difference between the police agents for both railroads is that Railroad B does attempt to physically conduct surveillance of many of the trains in transit, especially while they are moving through high-density areas. Additionally, Railroad B assigns agents to trains carrying sensitive and high-value targets while they are in transit. Railroad B often transports sensitive loads, such as military and government assets.

Railroad A moves significantly more tank cars and hazardous materials than Railroad B. This is simply due to the nature of the business and the geographical location of both rail lines within the area in which this study was performed. Both

railroad agents employed by Railroad A were adamant that tank cars hauling highly hazardous materials were not left unsupervised while in the custody of the carrier. The agents expressed concern about the tank cars once they were turned over to the company where delivery was made. It is at this time that the tank cars are no longer under Railroad A's immediate control and supervision.

Due to the nature and geographical location of Railroad A, the railroad is unable to reroute trains moving hazardous materials from high-density populated neighborhoods. Therefore, while in transit, the safest location to place tank cars is in the middle and toward the rear of the train (D'Amico 2006b; Plant and Young 2007). Time after time, this is where the investigator observed the tanks located in every train. The reason is, in the event of a crash or an explosion, the potential for penetration or destruction is reduced.

Railroad B ships considerably less tank cars and hazardous materials; consequently, it was more difficult to capture effective data for this project. The few tank cars that were observed were in the middle or toward the back of the train. The investigator did not observe any tank cars unattended on or near Railroad B's main line. Railroad B's agents stated that they remain vigilant and closely monitor any hazardous materials that are conveyed by their carrier.

As for the corporate security culture of the railroads, the final observation undertaken, the investigator found that the security agents employed by both Railroad A and Railroad B were dedicated, vigilant, and passionate about railroad safety, security, target hardening, and counterterrorism. With regard to the management and the general employees, those who worked outside the scope of security and law enforcement, the culture varied between Railroad A and Railroad B.

Clearly, during the investigator's direct observations, the employees at Railroad A took security more seriously than those employed by Railroad B. This conclusion is driven by several factors. The first factor is that the level of financial support that Railroad A provides is more significant, allowing for the best vehicles, equipment, and tools to be purchased. Railroad A's vehicles, firearms, and equipment were, for the most part, brand new and of the highest caliber. Railroad B operated older vehicles, did not have up-to-date equipment and computers, and were not compensated anywhere close to that of Railroad A's personnel and that of any law enforcement in the surrounding areas. Since the original direct observations took place, Railroad B has invested supplemental resources to upgrade vehicles and equipment.

Table 10.1 contrasts the key potential security risks between both of the selected railroads.

### **10.3.2 Direct Observations and Literature Review**

The threat of terrorism continues to evolve, constantly changing as the US counterterrorism methods advance. The enemy is always altering the plan of attack, trying to seize a moment when the United States is unprepared, using a different strategy, often unconventional in nature (Arquilla and Ronfeldt 1996). During this phase of the study, the data from the direct observations and the literature review came

**TABLE 10.1 Findings from Direct Observations**

Potential	Railroad A	Railroad B
Security risks	Class I (major)	Class II (regional)
Trespassing	Vulnerable	Vulnerable
Rail yard security	Insufficient	Satisfactory
Bridges (critical infrastructure)	Vulnerable	Vulnerable
Tank cars (highly hazardous materials)	Satisfactory	Satisfactory
Risk assessment	Satisfactory	Satisfactory
Cybersecurity threats	Satisfactory	Satisfactory
Corporate security culture	Satisfactory	Vulnerable
Law enforcement (security management)	Satisfactory	Satisfactory

together, hand in hand, revealing a plethora of modes that can be used to breach security and attack the American freight railroad system:

1. The high-profile nature of freight railroading and the thousands of miles of the accessible infrastructure create an environment at risk for a terrorist attack (Plant 2004; Plant and Young 2007). Even though the freight railroad system has been vulnerable for as long as it has existed, terrorism has transformed how the entire transportation system operates, and stakeholders have a responsibility to public safety by implanting a security program that will decrease their vulnerability (Griset and Mahan 2003).
2. The capability of terrorists to target hazardous materials being shipped in tank cars to trigger a catastrophic incident remains a viable threat (Sullivant 2007). Toxic-by-inhalation chemicals are carried every day by freight railroads. Moreover, freight railroads are mandated by federal law to transport hazardous materials as freight railroading remains the safest mode for movement (Reed 2007). By using an unconventional method to derail tank cars, causing a breach where these chemicals may be released, makes the freight railroading method an appealing target. The vast geographical area that could be impacted and the rate of death that can result proliferate the threat (Sullivant 2007).
3. The threat exists to the American freight railroad system of weapons of mass destruction (WMD) being introduced through containerization that originated outside the United States and channeled onto freight trains (Szyliowicz 2004). The type of contraband that may be introduced is wide-ranging, including nuclear weapons, radioactive material, and conventional explosives. Due to the nature of the system, as tracks often traverse near major cities, dangerous contraband inside containers may be brought within a close proximity to high-density areas where an attack would affect significant populations, causing a catastrophic incident (Szyliowicz 2004).
4. The potential to facilitate cyberterrorism, hacking, and state-sponsored information warfare in order to breach the security of the American freight railroad system endures (Plant and Young 2007). Massive computer networks

regulate each aspect of the scattered system that comprises suppliers, customers, stations, yards, signals, points of interchange, railroad switches, bridges, and other carriers. All of these essential fixtures must work in sync in order to maintain everyone's safety and to avoid potential accidents or derailments (Plant and Young 2007). Moreover, an enemy could sabotage the supply chain, a railroad switch, a signaling device, or a bridge over water that could be deliberately altered with the intent to trigger a major derailment. Also, an enemy may try to gather sensitive security data to identify weaknesses and vulnerabilities in the carrier's system as the enemy plan an attack.

5. The threat to the food supply chain while in the custody of the American freight railroad system creates the potential for introducing contaminants into the food (Flynn 2004). A large amount of food products are transported via the American freight railroad system. Unlike other modes of transportation, the trains may sit idle and unsupervised for extended periods of time while being transported. Therefore, the opportunity for food contamination exists. According to Flynn (2004), the impact would be substantial as fear would resonate throughout the country. More than just the potential for death, the fact that security was breached and the food supply chain contaminated would be harmful to the entire population.
6. The lack of physical barriers protecting thousands of miles of railroad infrastructure from undetected trespassers on property owned by railroad carriers provides many opportunities to tamper with critical components of the railroad system (Plant and Young 2007). The ability of individuals to trespass throughout vast geographical areas of railroad infrastructure makes the entire system vulnerable to a major terrorist attack. Railroad property and items on railroad property are susceptible to criminal mischief and theft. Railroad engines, rolling stock, and bridges can be entered without immediate detection, creating an environment where the potential for security breaches and unconventional terrorist attacks remain an appealing goal for US adversaries (Plant and Young 2007).

### **10.3.3 Network Approach to Counterterrorism by Security Partners**

In response to the events that occurred on 9/11, the federal government and the entire railroad industry took numerous steps in order to improve security management and counterterrorism. A network approach was used by the many partners involved to advance the overall security of the industry (Plant and Young 2007). Here is an outline of the steps that were taken:

1. A comprehensive security plan was developed and implemented by the Association of American Railroads (AAR n.d.). The vast number of stakeholders involved in the industry, as well as those associated with homeland security, contributed to these security improvements. Comprehensive changes were made, especially with how US freight carriers shipped hazardous materials across the rails (Plant and Young 2007).

2. Transportation Information Sharing and Analysis Center (ISAC) was developed as a direct outcome of the changes implanted by the AAR (n.d.) after 9/11. ISAC emerged as the central agency for gathering, evaluating, storing, and propagating critical intelligence and information to the industry (Plant and Young 2007; U.S. Department of Homeland Security n.d.a). ISAC also shares threats and intelligence related to the transportation sector with the FBI National Joint Terrorist Task Force (JTTF) on an ongoing basis (U.S. Department of Homeland Security n.d.b).
3. The U.S. Department of Homeland Security developed legislation that required hazardous materials to be transported via the safest and most secure route available to the destination in which the materials are headed. Certain corridors were identified as high-threat urban areas (HTUA). These areas were those corridors located in close proximity to major cities with dense populations (D'Amico 2005; D'Amico 2006a, b; Plant and Young 2007; Reed 2007). Communities must also propose legislation mandating that toxic-by-inhalation chemicals are routed around their populated urban areas. When this is not viable, local first responders must be notified in the event of an incident.
4. Other measures that were taken following the events of 9/11 included the development and manufacturing of tank cars designed to be safer in the event of an explosion or derailment, the potential outcome of any terrorist or criminal attack. Some of the improvements that were made encompassed the development of safety platforms, nonoverriding couplers, and sturdier tank heads. Freight railroad carriers also started and continued placing tank cars in the middle and the rear of the train, a safer location in the event of a physical impact or fire (D'Amico 2006b; Plant and Young 2007).
5. The screening of containers prior to entering the United States became more prevalent in November 2011. The Customs-Trade Partnership against Terrorism (C-TPAT) was designed to identify high-risk containers that were at risk for terrorism. By detecting high-risk shipments as early as possible in the supply chain, the shipments can be stopped long before container contraband is introduced into the American freight railroad system (Fickes 2007; Szyliowicz 2004). One hundred percent of containers must be screened before they are funneled from the US ports to freight carriers. The screening may be completed through risk assessment or through physical screening depending on the threat level of the specific shipment.

Models are created to measure risk. The foremost threat is that a terrorist will embed a WMD inside a container while in a foreign country, and the WMD will be funneled into the freight railroad system. Several factors drive these models, including the specific foreign port that the containers are being forwarded from, the political environment in the country, and the level of security screening that is consistently done before the containers are allowed to be shipped to the United States (“Supply Chain Security,” 2013).

6. The safety and the security of the American freight railroad system were improved by the use of risk analysis. Risk analysis is instrumental in funneling

money toward the highest security needs. Because the railroad system is so large and decentralized, it is not realistic to place a wall and cameras around the entire railroad. Therefore, risk analysis helps to identify where they are truly needed and where the highest probability for a terrorist attack exists (GAO-04-598T: Rail Security 2004). Engineers also use risk-assessment techniques in the design of structures, tunnels, and bridges. The objective is to lessen the vulnerability for a security breach and terrorist attack, as well as to build in provisions to accommodate first responders (Spielvogel 2004).

7. Additional police patrols were implanted following 9/11 in an attempt to cordon off carrier-owned infrastructure and to decrease the prevalent culture where individuals feel they can trespass without any liability or significant penalty (Plant 2005; Plant and Young 2007). Furthermore, railroad carriers have invested in educating general employees outside the scope of security to be on guard for suspicious activity and trespassers. The goal is to train employees in what to look for and in what specific steps can be taken if they observe suspicious behavior. This will give them the tools that can challenge terrorist suspects before they have any opportunity to carry out an attack (Plant and Young 2007). The industry is also conducting awareness campaigns for “rail fans,” similar to traditional neighborhood crime watch programs. Additionally, railroad police agencies must coordinate security efforts with other municipal, county, and state agencies that have jurisdiction near and alongside their infrastructure.
8. The e-RAILSAFE program that began in 1999 was augmented following the events of 9/11. The insider threat remains one of the greatest risks for terrorist attacks against the American homeland’s transportation sector. Vetting and comprehensive background checks are performed on employees of vendors, contractors, and the railroad themselves before ID credential badges are issued for them to wear while on railroad carrier property. Furthermore, the chance for deception is reduced (e-Verifile.com, Inc. 1999–2013).
9. Freight railroads perpetually enhance network security systems to safeguard against persistent cyber threats. They constantly defend against intrusions by utilizing a multilayered risk-based methodology. The methodology includes security architecture, patch management, intrusion detection and prevention, firewalls, active monitoring, antivirus software, application security, data encryption, password policies, active process and exception management, education and security awareness, response and containment programs, and frequent assessments of vulnerabilities (Carlson, as cited in Sneider 2012). Additionally, the railroads recruit professional ethical hackers to attempt security breaches into their systems.

The Surface Transportation Information Sharing and Analysis Center (ST-ISAC) provides daily bulletins to railroads warning of susceptibilities associated with cybersecurity, software, and recommendations for managing these contemporary threats against their networks. The advisories, driven by

the latest intelligence, continually evolve as the hackers are always looking for new methods to breach the networks (U.S. Department of Homeland Security 2012).

Security management and counterterrorism have evolved since the earliest stages following 9/11. More importantly, the understanding and the culture of insiders, the decision makers, and the general public have greatly improved. This investigation sought to glean new ideas, descriptions, themes, interpretations, and assertions that can be utilized to improve security management surrounding the American freight railroad system in the future. These findings were a direct result of the direct observations and the literature review.

## 10.4 RECOMMENDATIONS

### 10.4.1 Recommendations for Improving the Security Management

1. Encroaching trespassers on railroad carrier property should be reduced. The nature of railroading and the absence of substantial barriers leave no alternative other than to expand the presence of security and law enforcement throughout carrier property and infrastructure. The amount of criminal mischief (graffiti) observed is clearly a strong indicator of how accessible the trains and the fixtures are to trespassers. Furthermore, all critical bridges and tunnels should have monitored alarms, surveillance cameras, and voice-over technology. Awareness campaigns (trespassing) and penalties for trespassers should be increased.
2. En route security should be increased in order to maintain the safety and the security of freight trains in transit. The level of railroad police agents should be parallel to other law enforcement organizations in order to provide a reasonable amount of security. High-risk shipments, sensitive shipments, and miscellaneous critical loads in transit should have added security and law enforcement to better manage the risk associated with these items being left unaccompanied for extended periods of time while in transit. Awareness of instructional campaigns for rail fans similar to traditional neighborhood crime watch programs also are imperative. The cost is nominal, and the additional eyes and ears are a tremendous benefit.
3. Railroad management culture should be changed, especially outside the scope of those who work in security management and law enforcement. Managers should provide reasonable resources needed to operate and maintain effective security. Upper managers must lead by example to create a security culture throughout the organization and demand that all employees remain vigilant. Carriers that do not have their own law enforcement agencies must strongly contemplate starting a force of sworn police officers.
4. Tank cars containing toxic-by-inhalation hazardous materials must be monitored throughout transit and while in the custody of the carriers. Moreover, once the materials are turned over to private companies, they must be properly secured and monitored to avoid any security breach or terrorist attack.

5. The inspection of containers should be increased, especially before the containers are funneled into the American freight railroad system. All companies that import cargo into the United States must be mandated to participate in the C-TPAT program. Railroad carriers also should perform risk-based inspections and screening.
6. Whistleblower protections should be increased for all employees with regard to security issues. Employees should be guaranteed that they will not face retribution from managers when they report legitimate gaps in security that jeopardize public safety. A user-friendly mechanism should be put into place by federal officials.

#### **10.4.2 Recommendations for Further Research**

Stakeholders should explore the impact of expanding railroad policing and presence in and along carrier-owned property. Statistics regarding benchmark items such as trespassing, graffiti, theft, and general incidents can be used to evaluate the difference that is made with the additional resources for target hardening. Research should continue for strategic funding strategies for increasing railroad law enforcement and security at all levels. Finally, research should be conducted on the risk of cyberterrorism, hacking, and state-sponsored information warfare that could negatively impact the railroad industry, both freight and passenger, by terrorists.

### **10.5 CONCLUSION**

The American freight railroading system is paramount to the American economy and is influenced by the global economy. Terrorist attacks against American homeland interests became more sophisticated leading up to 9/11 and have continued to become more perilous since 9/11. Whether successful in carrying out an assault or not, the enemy is always looking for different methods for causing destruction to the United States. An example of this is following the “planes operation.” Once the Transportation Security Administration developed more advanced methods to screen passengers, the enemy tried to attack the civil aviation system using explosives hidden inside shoes and in underwear. Therefore, it is vital to identify other infrastructure or, in this case, freight railroading that is susceptible to terrorist attacks.

The American freight railroad system is large, decentralized, and challenging to secure due to its breadth and inability to secure with physical walls. Countless miles of track, rail switches, bridges, and rolling stock are spread out throughout the United States. Additionally, major staples that Americans depend on, as well as highly hazardous materials, and other high-risk shipments continuously move all around the enormous system.

Deciding exactly how much to invest in target hardening and security management remains elusive and fluctuates depending on with whom you speak. According to Mueller and Stewart (2011), the Department of Homeland Security emphasizes what can occur prolifically as opposed to using actual risk as a gauge to budget security

management costs. The value of added security rests on the likelihood of an effective terrorist assault, as well as the losses that ensued, including both human life and monetary losses (Mueller and Stewart 2011).

This study was conducted to identify the specific security management challenges related to the American freight railroad system. Once recognized, the data that were collected assisted in pinpointing specific methods that can be deployed in order to initiate a major terrorist attack. Moreover, the best practices for securing the American freight railroad system following 9/11 were delineated, and many best practices were promulgated in this report. Realistic ongoing assessment is vital. Society, the carriers, and the many people who live near railroad infrastructure are impacted by the possibilities of an attack. The research contributes to social change by increasing the safety and the security of freight railroading and by protecting the American economy. The bottom line is, we must never forget that the United States was brought to its knees with box cutters on 9/11.

## REFERENCES

- Arquilla, J. & Ronfeldt, D. (1996). The advent of netwar (revisited). In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars* (pp. 1–28). Santa Monica, CA: Rand, National Defense Research Institute.
- Associated Press. (2009, July 2). *Italian train derailment death toll rises to 22*. Retrieved from [http://www.nytimes.com/2009/07/02/world/europe/02italy.html?\\_r=0](http://www.nytimes.com/2009/07/02/world/europe/02italy.html?_r=0) (accessed March 2, 2015)
- Association of American Railroads. (n.d.). *Freight rail security briefing*. Retrieved from <http://www.aar.org/~media/AAR/PositionPapers/Security.ashx> (accessed March 2, 2015).
- Barrett, J. M., Ritter, L. & Wilson, R. (2007). *Securing global transportation networks: A total security management approach*. New York: McGraw Hill.
- Capra, G. S. (2006, December). *Protecting critical rail infrastructure*, (Counterproliferation Paper, Future Warfare Series No. 38). Maxwell Air Force Base, AL: Air University, USAF Counterproliferation Center. Retrieved from [http://cpc.au.af.mil/pub\\_books.aspx](http://cpc.au.af.mil/pub_books.aspx) (accessed March 2, 2015).
- D'Amico, E. (2005, December 14). Philadelphia eyes hazmat rail transport. *Chemical Week*, 167(42), 8. Retrieved from EBSCO.
- D'Amico, E. (2006a, January 25). Moving through unfriendly territory. *Chemical Week*, 168(3), 17–19. Retrieved from EBSCO.
- D'Amico, E. (2006b, September 20). Transportation. *Chemical Week*, 168(2), 39–41. Retrieved from EBSCO.
- Daniels, R. (2000). *Trains across the continent: North American railroad history* (2nd ed.). Bloomington, IN: Indiana University Press.
- David, A. & Rizzo, A. (2009, June 30). *Associated Press*. Freight train derails in Italy, killing 13. Retrieved from <http://news.aol.com/article/freight-train-crash-italy/549175> (accessed March 2, 2015).
- Department of Homeland Security Reform Act of 2005, H.R. 4009, 109th Cong. (2005).
- e-Verifile.com, Inc. (1999–2008). e-RAILSAFE: The security and safety initiative of class I railroads. Retrieved from <http://www.e-railsafe.com> (accessed March 2, 2015).

- Fickes, M. (2007, April/May). Containing risk. *Government Security*, 6(2), 16–21.
- Flynn, S. (2004). *America the vulnerable: How our government is failing to protect us from terrorism*. New York: HarperCollins.
- GAO-04-598T: Rail Security. (2004). *Rail Security: Some actions taken to enhance passenger and freight rail security, but significant challenges remain* Hearing before the Committee on Commerce, Science, and Transportation, of the U.S. Senate, 108th Cong. (2004) (testimony of Peter G. Guerrero & Norman J. Rabkin). Retrieved from <http://www.gao.gov/new.items/d04598t.pdf> (accessed March 2, 2015).
- Griset, P. L. & Mahan, S. (2003). *Terrorism in perspective*. Thousand Oaks, CA: Sage.
- Guterman, S. (2010, April 4). *Blast derails Russian freight train-reports* (A. Williams, Ed.). Moscow: Reuters. Retrieved from <http://www.reuters.com/article/2010/04/04/idUSLDE63300Q> (accessed March 2, 2015).
- Jordan, G. & Reed, J. H. (2007, September). Using systems theory and logic models to define integrated outcomes and performance measures in multi-program settings. *Research Evaluation*, 16(3), 169–181.
- Karpov, E. A., Mokhorov, G. A. & Rodin, V. A. (2003, January/February). International terrorism and its military-political organizations. *Military Thought*, 12, 4–13. Retrieved from EBSCO.
- Mueller, J., & Stewart, M. G. (2011, August). Balancing the risks, benefits, and costs of homeland security. *Homeland Security Affairs*, 7(16). Retrieved from <https://www.hsaj.org/articles/43> (accessed March 2, 2015).
- Patton, M. Q. (2002). *Qualitative research and evaluation methods*, (3rd ed.). Thousand Oaks, CA: Sage.
- Plant, J. F. (2004, May). Terrorism and the railroads: Redefining security in the wake of 9/11. *Review of Policy Research*, 21(3), 293–305.
- Plant, J. F. (2005, Fall). Competing models for enhancing railroad security. *Public Manager*, 34(2), 13–19. Retrieved from EBSCO.
- Plant, J. F. & Young, R. R. (2007, June). *Securing and protecting America's railroad system: U.S. railroad and opportunities for terrorist threats*. Harrisburg: Pennsylvania State University, School of Public Affairs.
- Reed, J. B. (2007, October/November). Securing dangerous rail shipments. *State Legislatures*, 33, 38–40. Retrieved from EBSCO.
- Samuels, R. (2009, March 14). Train thief took a 120-ton joy ride. Miami, FL: Miami Herald Media Company, pp. 1–3.
- Sneider, J. A. (Ed.). (2012, September). Communication and signal article: Railroads gear up to protect computers from hackers. *Progressive Railroading*. Retrieved from [http://www.progressiverailroading.com/c\\_s/article/Railroads-gear-up--to-protect-computers-from-hackers--32354](http://www.progressiverailroading.com/c_s/article/Railroads-gear-up--to-protect-computers-from-hackers--32354) (accessed March 2, 2015).
- Spielvogel, L. G. (2004, November). ASHRAE homeland security activities and reports. *ASHRAE Journal*, 46, 34–36. Retrieved from EBSCO.
- Stevens, B. (2004). The emerging security economy: An introduction. *The Security Economy*. Paris: Organization for Economic Co-operation and Development.
- Sullivant, J. (2007). *Strategies for protecting national critical infrastructure assets: A focus on problem solving*. Hoboken, NJ: John Wiley & Sons, Inc.
- Supply Chain Security. (2013, September). *Supply chain security: DHS could improve cargo security by periodically assessing risks from foreign ports*. Washington, DC: United States Government Accountability Office.

- Szyliowicz, J. S. (2004, May). International transportation security. *Review of Policy Research*, 21(3), 351–368.
- U.S. Department of Homeland Security. (2012, May 31). *Written testimony of Howard R. "Skip" Elliott before the U.S. House of Representatives, Subcommittee on Transportation Security and Infrastructure Protection, Hearing on TSA's Surface Inspection Program*. Retrieved from <http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg78155/html/CHRG-112hhrg78155.htm> (accessed March 2, 2015)
- U.S. Department of Homeland Security. (n.d.a). *Transportation Security Administration: Freight Rail Modal Annex*. Retrieved from [http://www.dhs.gov/xlibrary/assets/Transportation\\_Freight\\_Rail\\_Modal\\_Annex\\_5\\_21\\_07.pdf](http://www.dhs.gov/xlibrary/assets/Transportation_Freight_Rail_Modal_Annex_5_21_07.pdf) (accessed March 2, 2015).
- U.S. Department of Homeland Security. (n.d.b). *Transportation Security Administration: Rail security*. Retrieved from <http://www.dhs.gov/blog/2009/03/04/partnership-key-reducing-risk-rail> (accessed March 2, 2015).
- U.S. Department of Transportation. (n.d.a). *Federal Railroad Security Administration*. Retrieved from <http://www.fra.dot.gov/Page/P0001> (accessed March 2, 2015).
- U.S. Department of Transportation. (n.d.b). *Federal Railroad Administration: Class I railroad*. Retrieved from <http://www.fra.dot.gov> (accessed March 2, 2015).
- U.S. Department of Transportation. (n.d.c). *Federal Railroad Administration: Class II Railroad*. Retrieved from <http://www.fra.dot.gov> (accessed March 2, 2015).
- Vlahos, K. (2008, March). A safer home on the range. *HS Today*, 5(3), 42–47.
- Von Bertalanffy, L. V. (1968). *General systems theory: Foundations, development, applications*. New York: George Braziller.
- Yin, R. K. (2003). *Case study research design and methods* (3rd ed.). Thousand Oaks, CA: Sage.
- Zengerle, J. (2001, November 19). Infinite justice. *New Republic*, 225(22), 17–20. Retrieved from EBSCO.

---

# 11

---

## COST-EFFECTIVE AIRPORT SECURITY POLICY

ROBERT W. POOLE, JR.

*Reason Foundation, Los Angeles, CA and Washington, DC, USA*

### 11.1 INTRODUCTION

In response to the 9/11 attacks, governments in the United States, Canada, and Europe (at both national and EU levels) added various aviation security measures to those that already existed. Most of these were aimed directly at preventing a repeat of that kind of suicide mission, in which a plane is hijacked and used as a missile. Among the new measures were strengthened (and locked) cockpit doors, 100% screening of checked baggage, more thorough screening of passengers and their carry-on baggage, increased use of onboard security officers, increased attention to air cargo, and greater attention to airport access control and perimeter control.

Although we hear lots of rhetoric about risk assessment and claims that security policies are “risk based,” the actual policy changes seem mostly driven by political imperatives to reassure frightened populations that air travel was still safe. The initial hastily enacted US legislation was called the Aviation and Transportation Security Act (ATSA), and it created the Transportation Security Administration (TSA) nominally to protect all of transportation. In fact, however, Congress has directed the vast majority of the TSA’s budget to *aviation* security (with by far the largest share concentrated on passenger and baggage screening). No risk assessment preceded this statute’s enactment, nor has this initial allocation of resources changed significantly after the TSA became part of the newly created multimission Department of Homeland Security (DHS).

One of the most important principles taught in basic economics is “opportunity cost.” What this means is that resources are always limited and that resources allocated to X are not available for Y. Accordingly, the challenge in dealing with terrorist threats—whether to a nation, a sector such as transportation, or a subsector such as aviation—is always one of deciding where to invest scarce resources to maximum benefit. This inevitably requires difficult choices to be made, and the premises of this paper are (i) that risk assessment provides an essential framework for making security choices and (ii) that such risk assessment should be applied far more rigorously to aviation security.

## 11.2 ANALYZING AVIATION SECURITY MEASURES

### 11.2.1 Unique Challenges Posed by Terrorism

The sector-specific approach that has been applied to aviation is an example of target hardening. The problem with this approach is that we live and function in a target-rich world; this is inherent in the nature of developed economies. Because resources are limited, all conceivable targets cannot be hardened. But when some targets are hardened, terrorists can readily shift from hardened to nonhardened targets. Target hardening is an example of what analysts have called “asymmetries” between terrorists and their target governments. Because terrorists can hide among the general population, they present a target-poor environment to governments, compared with the terrorists’ target-rich environment. And the cost to terrorists of wreaking destruction and creating fear are modest, in comparison to the costs of governmental attempts to defend (everything) against terrorist attack.

In a 2008 Copenhagen Consensus “challenge paper” on terrorism, Sandler, Arce, and Enders discuss why doing benefit/cost (B/C) analysis is so difficult in the case of counterterrorism efforts (Sandler et al. 2008). First, there is no permanent solution to terrorism, so benefits from a counterterrorist strategy are likely to last (they guess) only 2–5 years. Second, there is no reliable way to know what level of terrorist activity there would be in the absence of the strategy. Third, the cost of such a strategy is difficult to ascertain, since much relevant information is classified.

The monetary benefits of preventing a terrorist act can be quantified as the value of lives saved and injuries prevented, the amount of property damage averted, and the avoided reductions in gross domestic product (GDP). Because terrorist incidents are infrequent and (thus far) of relatively small impact, in B/C calculations, the security expenditure, as a fraction of GDP, dwarfs the other variables over a wide range of assumed values for the parameters. Overall, Sandler et al. conclude that “security-based solutions display adverse B/C [ratios]” and that it would be better to shift to low-cost strategies based on greater international cooperation and changed foreign policy.

An important caveat to this assessment was discussed in a companion paper (Intriligator 2008). Sandler et al. do not factor in possible terrorist use of biological, chemical, radiological, or nuclear materials, since their estimates of lives lost, injuries

sustained, and reductions in GDP are based on historical transnational terrorist activity, none of which has involved these more serious threats. Had data been available to quantify such costs, the B/C ratios for several of the strategies would have been “much larger,” as Sandler et al. concede. This is not very relevant for this chapter because aviation does not appear to be a current target for such weapons.

A summary of the 2008 OECD/International Transport Forum Round Table on Security, Risk Perception, and B/C Analysis drew an important distinction between *safety* analysis and *security* analysis (International Transport Forum 2009). Safety is concerned with *risk*, while security is concerned with *uncertainty*. In analyzing safety risks, the events involved are unintentional and there is generally a reasonably large dataset from which to estimate probabilities. By contrast, security events are intentional and are far fewer in number, such that “no credible objective probability can be assigned to their occurrence.” After reviewing a number of possible sources of probability estimates, the summary concludes that while “no objective probabilities can be determined for the occurrence of attacks,” subjective probabilities “can be gleaned from intelligence, the insurance industry, and prediction markets” even though this is not currently being done systematically in security policy-making.

### 11.2.2 How to Use Cost-Effectiveness Analysis in Aviation Security

Although traditional *B/C* analysis of antiterrorist measures is difficult, for the reasons outlined previously, there are other approaches to assessing the value of security measures. Stewart and Mueller analyzed several components of the TSA’s aviation security program in the United States (Stewart and Mueller 2008). In this paper, they did not attempt to make *B/C* ratio calculations, as in the Copenhagen Consensus paper discussed previously. Instead, Stewart and Mueller assessed the *relative cost-effectiveness* of several measures, using as a metric the cost per life saved. This approach has been used extensively in studies of the relative cost-effectiveness of safety-related regulatory measures. A table in their report draws on regulatory analyses of measures enforced by six US safety regulatory agencies (including the Federal Aviation Administration (FAA)). The annual cost per life saved (in 1995 dollars) ranged from a low of \$0.1 million for FAA’s aircraft cabin fire protection standard to a high of \$6.78 trillion for EPA’s hazardous waste listing for wood-preserving chemicals. In reviewing possible safety regulations, the US Department of Transportation uses a figure of \$3 million per life saved as a ceiling for acceptable regulatory costs.

Stewart and Mueller identified 20 TSA aviation security efforts, 14 that deal with security at the airport (mostly concerning passenger and baggage screening, but also access control and other factors) and six that deal with in-flight security. They grouped the six in-flight measures into three: crew and passenger resistance, hardened cockpit doors, and federal air marshals (FAMs). Consistent with current thinking among aviation security professionals, they assumed that in-flight efforts have made a considerable difference in reducing the probability that a plane will be hijacked and turned into a weapon. Hence, their starting assumption was that the in-flight measures

account for 50% of the reduced risk of a 9/11 aircraft takeover, with the 14 preboard security measures adding up to the other 50%. And as another initial assumption, they assumed that the three in-flight measures are each equally effective—that is, each accounts for 16.67% of the total reduced risk. They then factored in a generous 10% probability that FAMs will be present on any particular plane. That reduces the risk reduction due to FAMs alone to 1.67%.

Stewart and Mueller postulated that in the absence of all those measures, there would be a 9/11 repeat (with approximately 3000 deaths) once every 10 years. Hence, they assumed this set of measures prevents an average of 300 deaths per year in the United States. From there on, it was a simple matter of doing the math, using the best available information on the annual costs of each measure. Two of the results they presented for the annual cost per life saved are as follows:

Hardened cockpit doors:	\$800,000
Federal air marshals:	\$180,000,000

Because several of their assumptions are somewhat arbitrary, they followed this with a sensitivity analysis. After varying the probability of success of each measure, they found that the general results in terms of relative cost-effectiveness held true over a wide range of assumed probabilities. They concluded that “even an order of magnitude reduction in the effectiveness of hardened cockpit doors (resulting in a cost per life saved of \$8 million) would not change the conclusion” that the cockpit doors are a far more cost-effective measure than air marshals.

In a paper for the OECD’s International Transport Forum, Poole applied Stewart and Mueller’s methodology to preboard security measures (Poole 2009). Using their assumption that 50% of the reduced risk of a 9/11 attack is due to the preboard measures, Poole used their basic equation:

$$C_{ls} = \frac{C_r}{L_s}$$

where  $C_{ls}$  is the annual cost per life saved,  $C_r$  is the annual cost of regulation r, and  $L_s$  is the annual number of lives saved due to regulation r. According to Oster and Strong (2008), about \$4.7 billion of TSA’s annual \$6.7 billion budget is spent on airport-related security (excluding cargo security). Using that figure for  $C_r$  yields an estimated cost of \$31.3 million per life saved, thanks to the set of preboard airport security measures—more than 10 times the US DOT standard and 39 times as great as hardened cockpit doors.

This approach obviously has its limitations, since it depends critically on assumptions about annual lives saved. But since reasonably good cost data exist, the calculations can be carried out for a range of lives saved assumptions. This kind of sensitivity analysis makes it possible to estimate the *relative* cost-effectiveness of various aviation security measures over a range of possible assumptions about security event frequencies.

In another paper, Stewart and Mueller illustrated a form of *B/C* analysis that lends itself to this kind of security measures evaluation (Stewart and Mueller 2011). The focus of this exercise was the introduction of body scanners by the TSA. They estimated the cost of a successful attack on an airliner with body-borne explosives (the threat body scanners are intended to counter) as \$26 billion. Their estimate of the annualized ownership and operating cost of a system of 1800 body scanners was \$1.2 billion. The question was then posed as: What does the yearly probability of a successful attack via body-borne explosives have to be to justify spending \$1.2 billion per year to reduce this risk by 7.5%? Their derived answer was 61.5% a year. That means that only if an attack is over 60% likely to occur and succeed in a given year, without the body scanner program, would it be worth spending \$1.2 billion per year to prevent it. They also subjected this calculation to sensitivity analysis to test its robustness. A further conclusion was that “the attack probability needs to exceed 160–330% per year to be 90% certain that [body scanners] are cost-effective.”

These examples illustrate that it is feasible to quantify the *relative* effectiveness of various aviation security measures, so as to make assessments of how to most productively allocate a given aviation security budget. There is little evidence in reports on TSA programs by the DHS Office of Inspector General or the Government Accountability Office (GAO) that such quantitative analysis has been applied to TSA decision making about aviation security policies or programs.

## 11.3 HOW RISK BASED ARE CURRENT SECURITY POLICIES?

### 11.3.1 International Aviation Security Standards

The International Civil Aviation Organization (ICAO), an affiliate of the United Nations, provides standards and recommended practices that all member states (signatories to the Chicago Convention) are expected to follow. ICAO’s Annex 17, *Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, sets forth the minimum aviation security standards expected of all member states (ICAO 2006). It requires each state to have a civil aviation security organization and a written aviation security program, as well as requiring each airport and airline to have a written security program. Supplementing Annex 17 is the *Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference*, commonly referred to as ICAO DOC 8973. It provides detailed procedures and guidelines on how states may go about implementing the provisions in Annex 17, but it is guidance, not a standard.

Standard 3.1.3 of Annex 17 states that each contracting state “shall keep under constant review the level of threat to civil aviation within its territory, and establish and implement policies and procedures to adjust relevant elements of its national civil aviation security program, *based on a security risk assessment carried out by the relevant national authorities*” (emphasis added). As interpreted by a review of Canada’s post-9/11 security agency Canadian Air Transport

Security Authority (CATSA), this establishes two basic principles for aviation security policy:

- “[I]t must be intelligence-led, based upon up-to-date threat assessments and resilient enough to adapt to new threats as they emerge.”
- “Risk analysis and assessment are the basis for effective use of security resources” (Advisory Panel 2006).

While this might sound like an invitation to use performance/outcome measures, Annex 17 goes on to prescribe input standards for preboard screening of passengers and baggage, the quality of screeners and periodic testing of them, passenger–bag reconciliation, cargo security controls, access control via secure identification and random screening, and airport perimeter control. Other Annexes provide for secured cockpit doors, procedures for dealing with disruptive passengers, and air marshals. These are all standards specifying inputs, all of which are assumed necessary regardless of any findings of risk analysis and cost-effectiveness analysis.

Thus, while the ICAO Annexes seek to ensure that at least minimum attention is given to all of these areas, there is potential tension between the implication that various inputs and methods *must be used* and the directive that decisions should derive from risk analysis based on up-to-date intelligence.

### 11.3.2 Canada’s Aspirations for Risk-Based Policy

The aforementioned review of CATSA includes a section called “Risks and Layers: Envisioning Aviation Security.” It cites the ICAO rhetoric and notes that “[Security] resources, financial and human, are not unlimited and should be allocated according to assessed risk” (Advisory Panel 2006). It notes that Canada’s Auditor General the previous year had insisted that a risk-based approach is desired and expressed disappointment that Transport Canada “has not fully implemented formal risk management” (Auditor General of Canada 2005). The Advisory Panel report goes on to say that in its presentations to the Panel, “CATSA referred to its concept of security screening as risk-based” and that “Priorities must be established, and these should be based on assessments of the relative level of risk.”

But industry stakeholders, such as airports and airlines, told the Panel that CATSA should follow a more seriously risk-based approach. For example, in passenger screening, the agency should “focus on higher-risk passengers, rather than on the objects carried by all passengers.” They also called for better background vetting, so as to streamline the screening that takes place at the airport, “such as a Registered Traveler (RT) program.” The submission by the Canadian Airports Council (CAC) used stronger language, saying that the current “one size fits all approach wastes precious resources” (Canadian Airports Council 2007). CAC urged that CATSA move to “a standard that allows different levels of screening at sites and between sites based on risk assessment criteria” and also recommended that an RT program be implemented.

According to an interview with the chief executive of CAC, as of late 2008, none of the changes the organization recommended had been implemented, but he believed that

risk-based changes were coming, with ICAO encouragement (Facette J. and Canadian Airports Council 2008, Robert Poole telephone interview, October 8). An April 2013 interview with that person's successor suggests that Canada's aviation security program is becoming more solidly based on threat assessment and risk assessment while providing greater scope for airports to tailor their risk mitigation efforts to the specifics of their facilities (Phelan C. and Canadian Airports Council 2013, Robert Poole telephone interview, April 15). A new National Civil Aviation Security Program (NCASP) document was released on April 4, 2013, defining risk management and illustrating how it will be applied in aviation security. As discussed later in this chapter, changes are also in the works for something like a Trusted Traveler (TT) program at the screening checkpoint.

### 11.3.3 Europe's Steps toward Risk Assessment

No EU-wide aviation security policy existed until 2002, when the European Parliament and Council agreed upon Regulation No. 2320/2002 establishing common rules for civil aviation security. Those regulations were revised substantially in 2008, with Regulation No. 300/2008 repealing and replacing the 2002 regulation. Consistent with ICAO Annex 17, each member state of the EU must have an NCASP, with a single agency in charge. The objective of No. 300/2008 is to provide a "common interpretation of Annex 17" within Europe (Regulation (EC) No. 300, 2008).

EC No. 300/2008 is still mostly prescriptive along the lines of ICAO Annex 17. But the fourth section of Article 4 permits EU member states to "adopt alternative security measures that provide an adequate level of protection on the basis of a local risk assessment." This wording implies that alternative approaches may be implemented if justified by risk assessment and possibly by cost-effectiveness analysis.

According to European airport and airline groups, efforts to implement a truly risk-based system are at an early stage within the EU. In October 2006, the Airports Council International Europe and the Association of European Airlines created a joint effort "to address shortcomings of the current system" (Airports Council International-Europe 2006). In its news release announcing the launch of the European Strategic Partnership for Aviation Security (ESPAS), the Director General of ACI Europe said that "Any new security rule should focus specifically on the threat or risk that needs to be eliminated, taking account of the impact on passenger mobility and convenience, operations, and cost." Industry sources portray the replacement of EC No. 2320/2002 with No. 300/2008 as a step toward a more flexible and better-harmonized aviation security system within Europe. The online publication HomelandsecurityEU.com commented, "From an industry standpoint, the inclusion of risk assessment is the key element of the new regime. By ensuring that the new security measures deriving from the framework are risk-based, each party will fully accept its responsibilities and its role in the security chain" (Homeland Security 2007).

However, as of late 2008, the Policy Manager for ACI Europe stated that "We are still in the early process of a truly risk-assessment-based system in aviation security in the EU" (Olteanu 2008, ACI Europe, email to Robert Poole, October 28). There is little public evidence of substantial change since then.

### 11.3.4 The United States: A Partial Shift toward Risk-Based Policy

The TSA is one of the many agencies that are part of the DHS. In 2005, DHS's then-Secretary Michael Chertoff announced a sweeping reorganization of the agency, shifting to what appeared to be a more risk-based approach to security. The former Inspector General of DHS, Clark Kent Ervin, praised the new approach as "a threat-based, risk-based, consequence-based approach." And then-new TSA Administrator Kip Hawley said that "The federal government must focus resources on the basis of consequences, threat and vulnerability assessments, and the prioritization of risks" (Business Travel News 2008).

In the first 3 years since those statements were made, very little evidence of risk-based policy change emerged from the TSA. In an August 2007 report on DHS's progress in implementing its mission, the GAO assessed the department's progress in aviation security as "moderate" and said that "Th[e] lack of a comprehensive strategy and integrated management systems and functions limits DHS's ability to carry out its homeland security responsibilities in an effective, risk-based way. DHS has also not yet fully adopted and applied a risk management approach," although the TSA had taken some steps in that direction (Government Accountability Office 2007). In June 2008, GAO published a summary of a forum in which 25 experts discussed the issue of applying risk management by DHS member agencies (Government Accountability Office 2008). They considered the Coast Guard (but not TSA) to be one of the few federal DHS agencies that had effectively incorporated risk management principles into its decision making; they also suggested that responsibility for risk management has been so distributed as to inhibit coordination on overall security priorities.

The one area where TSA has made visible progress on risk-based policy is TT. When the idea was first introduced to the aviation security community shortly after 9/11, it was presented as a risk-based program that would lead to better allocation of airport screening resources, by permitting those who had been "prescreened" to receive a lower level of scrutiny at the checkpoint (Levine and Golaszewski 2001). But the "RT" program that TSA allowed to be launched by private provider companies did not provide expedited checkpoint screening. TSA Administrator Kip Hawley believed that carefully selected "sleeper" terrorists could infiltrate the program, so he refused to allow expedited screening. But that position was incoherent because TSA also refused to permit RT applicants' data to be submitted to the Federal Bureau of Investigation (FBI) for a criminal history background check, as the companies had intended. Without that background check, TSA had insufficient basis for giving RT members expedited screening, allowing Hawley to repeatedly describe RT as follows: "It's not a security program but an ID [identification] program" (Business Travel News 2008).

That policy has been altered by Hawley's successor, John Pistole. He embraced a form of the original TT concept, implementing it beginning in late 2011 as PreCheck. Travelers who could be shown to be long-time frequent flyers with a particular airline and who are not on government watch lists could join the program, as selected by participating airlines. TSA created separate PreCheck screening lanes at major airports (40 airports as of mid-2013), offering what amounts to pre-9/11 screening for those travelers: no need to remove shoes, jackets, or overcoats, and no need to remove laptops or cosmetics from carry-on bags.

Well before the development of PreCheck, US aviation stakeholders and TSA worked together to devise ways of analyzing the costs and benefits of various aviation security policies. By late 2005, TSA concluded that it needed a “revolutionary” approach to understanding the risks involved in aviation and ways of quantifying the risk reduction potential of various countermeasures. As an outgrowth of such discussions, Boeing Company in 2007 began developing for TSA a prototype Risk Management Analysis Tool (RMAT), the specifics of which are classified. According to a recent RAND Corporation assessment, RMAT is in use today “to estimate the risk-reduction benefits attributable to new and existing security programs, technologies, and procedures” (Morral et al. 2012). RAND’s 2012 assessment found that while RMAT has improved TSA’s understanding and use of risk assessment, such a complex “high-resolution” model depends critically on estimated values for numerous parameters, many of which are either unknown or are produced as estimates that have a wide range of possible values. Its report suggests that TSA develop a simplified, low-resolution model that could “highlight the key sources of uncertainty affecting outcomes and then use exploratory analysis to evaluate the space of possible future outcomes”—analogous to the kind of planning the Department of Defense now does in its Quadrennial Defense Review.

## 11.4 TOWARD A MORE RISK-BASED APPROACH

As we have seen, aviation security officials in Canada, Europe, and the United States have all professed the importance of risk assessment as an important tool for allocating limited resources to protect civil aviation from terrorist attacks. But thus far, there is little evident use of such assessment in making judgments about which current policies are worth their costs. Independent analysis has suggested very poor cost-effectiveness for air marshals, but the United States has retained the FAM program unchanged. All the countries under consideration in this chapter have adopted the cost-effective measures of strengthening cockpit doors and changing the protocols by which flight and cabin crew deal with attempts to commandeer an aircraft in flight. Other studies have suggested that the US Federal Flight Deck Officer program that trains volunteer airline pilots and first officers to be armed in flight (as many pilots routinely were during the 1950s and 1960s) is far more cost-effective than FAMs, but that low-budget program has not been expanded, by Congress, at TSA’s request (Stewart and Mueller 2013). However, since the large majority of aviation security spending is for programs on the ground, our focus in this section is on crafting a more risk-based and cost-effective set of *airport* security measures.

### 11.4.1 Risk-Based Passenger and Baggage Screening

For the most part, current screening practices are very similar in Canada, Europe, and the United States. And given the extensive travel among these jurisdictions, reasonably consistent policies make good sense. The major change entailed by the proposed risk-based approach would be to alter the present de facto policy of treating nearly all

passengers and bags as needing equal scrutiny. Instead, the system would be based on applying somewhat different procedures to different categories of passengers and their bags, based on an assessment of their relative riskiness.

The basic approach was outlined in this author's 2006 paper on risk-based airport security (Poole 2006). Its premise is that the task of airport screening should be to identify and isolate dangerous *persons*, not dangerous *objects*. The challenge is to keep those persons from causing harm, either in the terminal area or to the planes themselves. There are many ways in which terrorists can cause great harm in connection with airports: getting on board with the aim of hijacking, getting on board as a suicide bomber, putting explosives into checked luggage or belly cargo but not getting on board, or targeting large concentrations of passengers in terminals. Current policies devote the major share of airport security resources to just two of these threats: preventing would-be hijackers from boarding with weapons and preventing such persons from boarding with concealed explosives. In fact, strengthened and locked cockpit doors (along with changed protocols for how crews deal with hijack threats) have greatly reduced the hijack threat. Body scanners are intended to thwart would-be suicide bombers, but as noted previously, it is hard to justify the cost of using them for all passengers, regardless of risk.

Far less money and effort are spent on securing airport terminal lobby areas and the ramp area where planes park. Thus, current policy, in effect, downplays the threat of bombers targeting crowds at checkpoints and lobby-based baggage screening installations and the threat of bombs being smuggled onto planes from the ramp (as opposed to the terminal).

The proposed risk-based approach would shift the focus to identifying dangerous people. This could include greater security guard presence in terminal lobby areas and outside the terminal, in ramp areas, and around the airport perimeter. And within the terminal, at the checkpoint, it requires separating passengers into at least three defined groups, based on the quantity and quality of information about each:

- Low-risk passengers, about whom a great deal is known
- High-risk passengers, based either on no knowledge or on specific, negative information
- “Ordinary” passengers, mostly infrequent flyers and leisure travelers, about whom much less is known than about those who have passed a background check, but who present no known risk factors

A different approach to both passenger screening and bag screening would be applied to each group.

*Low-risk passengers* are defined as those who possess a current government security clearance or who have been accepted into a TT program by passing a background check and being issued a biometric identity card. Passengers in this group would go through express lanes at checkpoints, with something like pre-9/11 protocols (no shoe or jacket removal, not having to remove laptops or other electronics, etc.)—essentially the screening currently provided to PreCheck members

at several dozen of the largest US airports. Their checked bags would not routinely be screened by explosive detection system (EDS) X-ray machines. The point is to not waste the system's limited resources or those passengers' time on procedures that add very little value to security. As a safeguard against the small probability that a dangerous person might slip into this category, a certain percentage of these people and their bags would be randomly selected for "ordinary passenger" screening, and this policy would be well publicized.

*High-risk passengers* include both those on watch lists (but not No-Fly lists, who would be either detained or denied entry to the checkpoint) and also those with little or no paper trail, about whom so little is known that the safest thing to do is to assume the worst and do a thorough screening of person and bags (both checked and carry-on). Everyone in this group, in other words, would receive a more rigorous version of today's "secondary" screening, to include both explosive detection scanning of their bags and either body scanning to detect nonmetallic objects or a thorough pat-down search.

*Ordinary passengers* are those in between the other two risk categories. These people would receive something like today's level of passenger screening (but with a better-justified list of banned objects and without routine body scanning). A fraction of this group would be randomly selected for secondary screening, as described previously.

This basic three-part division of passengers was adopted by the International Air Transport Association (IATA) in 2011 for its Checkpoint of the Future concept. During 2012, the organization conducted trials of component technologies at Geneva, London Heathrow, and Amsterdam Schiphol Airports, and it plans further technology demonstrations during 2013 (Lo 2013).

#### 11.4.2 Identifying Low-Risk Passengers (TT Programs)

Levine and Golaszewski suggested the idea of separating out low-risk travelers and expediting their processing at airports in an article published two months after 9/11 (Levine and Golaszewski 2001). Frequent flyers would apply to national aviation security authorities for membership by submitting to a background check, equivalent to a low-level security clearance. Those who passed this one-time screening would obtain a biometric identity card, and when they used the card at the airport to prove they were the person who had been cleared, they could bypass the more stringent post-9/11 screening.

The concept was first subject to detailed analytical scrutiny by a team of graduate students in operations research at Carnegie Mellon University in 2003 (Foster et al. 2003). They first created a model of passenger checkpoint processing, based on data from Pittsburgh International Airport (PIT). Next, they created a design for a TT program called SWIFT and simulated its operations using the model. Based on data from two surveys of airline passengers, they estimated that 40% of a typical day's worth of originating passengers would sign up for and be accepted into the system (mostly frequent business travelers). Based on their simulation, first-class and elite

frequent flyers (who already had a priority line at PIT) would see their average throughput time cut nearly in half, from 2.5 min down to 1.35. Coach passengers joining the program would have their average time slashed from 19.5 to 1.35 min. But those still using the regular lanes would benefit also. Since 40% fewer people would be using the regular lanes, their average processing time would drop from 19.5 to 12.1 min. The paper estimated that first-year benefits would exceed first-year costs by \$2 million at PIT.

The RAND Corporation subsequently estimated that a protocol that would exempt TTs from the mandate for 100% screening of their checked baggage via EDS would reduce the number of these costly machines required nationwide by approximately one-half (Shaver and Kennedy 2004). That approach would produce large dollar savings in both capital costs (when current machines have to be replaced) and staffing costs.

As noted in the previous section, when TSA allowed “RT” to be introduced, the only background check it carried out was to check applicants against its watch list—the same procedure applied to every air traveler prior to issuance of their boarding pass. Understandably, this was inadequate for allowing RT members to get less screening at the checkpoint than other air travelers. TSA at that time implied that the cost of a “real” background check would be prohibitive. Yet several million US aviation workers have been subjected to FBI criminal history background checks since 9/11, as a condition of being allowed access to secure areas of the airport (passenger terminals beyond security checkpoints, ramp areas, hangars, etc.) on a regular basis. This program is operated by the American Association of Airport Executives (AAAE), in cooperation with the FBI, at a cost of \$27 per person (American Association of Airport Executives, n.d.). At nearly all US airports, such airport workers do not have to pass through metal detectors or have their tools X-rayed when entering secure areas. In fact, from the inception of the RT program, the certified RT companies sent the fingerprints of all applicants to the AAAE clearinghouse, but TSA never gave permission for these 200,000 sets of prints to be sent to the FBI for the expected criminal history background check (Morris C. and American Association of Airport Executives 2008, Robert Poole telephone interview, November 10). Thus, a background check that TSA deems sufficient to allow unescorted and unscreened airport workers access to planes was deemed insufficient to allow RT members to pass through a streamlined version of checkpoint screening, as envisioned in the original TT concept.

The TSA’s current PreCheck version of TT does offer expedited screening. But it requires neither a criminal history background check nor a biometric ID card and as therefore not as secure as it should be. This is ironic, since for several years preceding the launch by TSA of PreCheck, its sister agency within DHS—Customs and Border Protection—has offered a TT program for expedited reentry to the United States from abroad at major airports. Global Entry requires an FBI background check and a biometric ID card. TSA accepts Global Entry as an alternative to airline nomination based on frequent flyer history.

Canada has begun creating separate airport screening lanes for holders of the Canada/US NEXUS cards, which permit these prescreened travelers to get faster

processing when crossing the land border between the two countries. The CAC director expects that Transport Canada will soon permit PreCheck-type faster screening for those using NEXUS lanes, which will include Global Entry members as well (Phelan C. and Canadian Airports Council 2013, Robert Poole telephone interview, April 15).

#### **11.4.3 Separating Ordinary and High-Risk Passengers**

Once low-risk passengers have been self-selected out of the mix, the remaining task is to use all feasible information to separate high-risk passengers from all the rest. One tool for doing this is a government-maintained watch list, continuously updated, against which all airline passenger reservations would be checked by the national aviation security agency in real time. In the United States, an updated program to do this was implemented in 2009, under the name Secure Flight.

A second approach is to assess what is known about each passenger, based on information provided at the time of ticket purchase. In the United States until 2009, this was carried out by the Computer Assisted Passenger Prescreening System (CAPPS), which dated from pre-9/11 days. The idea of such risk screening systems is to use various algorithms to (i) verify the passenger's identity and (ii) look for patterns that might suggest high risk. CAPPS used, and Secure Flight uses, algorithms to flag some passengers for secondary screening.

To supplement the previous tools and to deal with lobby-area persons not holding tickets (and therefore not passing through the screening checkpoints), precheckpoint lobby areas should be continuously monitored by some combination of video surveillance, plain-clothed security people, and uniformed police officers. These techniques are routine in Las Vegas casinos and also at Israeli airports (Davis et al. 2002). The general idea is to unobtrusively monitor people's behavior, looking for suspicious activities, to be followed up by questioning by security personnel. Many other airports maintain, at their own expense, either covert or highly visible law enforcement patrols within airport premises, including lobby areas and airside areas.

#### **11.4.4 Redesigning Passenger Checkpoints**

Security checkpoints for a risk-based system would be different from those at today's airports. First, there would be two different sets of lanes, one set for TTs and another set for all others. The proportion of each would have to be varied over time, depending on the fraction of daily originating passengers who were TT program members. Space would be required on the approach to the TT lanes for kiosks at which members would insert their biometric identity cards to gain admission to the line for these lanes. These kiosks might be combined with common-use boarding pass kiosks, saving TT members without checked baggage from having to stop at two different kiosks.

On the "sterile" (past screening) side of the checkpoint, additional space would be required for secondary screening portals to check the bodies and carry-on bags of selectees for explosives and potential weapons. All high-risk passengers (except those on the No-Fly list, who would be detained) would automatically go through

secondary screening. Boarding passes would be coded electronically, not visibly, so that a selectee would not know whether he/she had been selected by an algorithm or at random.

Meeting this set of criteria may require somewhat more square footage than is now allocated for checkpoints, though this will vary from airport to airport. On one hand, added space would be needed for TT kiosks and for expanded secondary screening equipment for selectees. On the other hand, significant TT enrollment should reduce the length of all waiting lines (and hence reduce the area needed for that purpose). And a smaller total number of selectees (thanks to more precise identification of people leading to fewer false positives in checks against watch lists) would lead to a smaller secondary screening area than if current percentages of passengers continued to be selected.

#### 11.4.5 Redesigning Checked Baggage Screening

Neither Canada nor most European countries require 100% of all checked baggage to be scanned by costly EDS machines. But where that mandate applies (as in the United States), the risk-based model would reduce the size and cost of checked baggage screening. The bags of TT members could be screened via two-dimensional X-ray machines and would only move on to the more costly screening if a possible problem was detected by the initial X-ray. RAND Corporation has done a number of studies of the impact that a TT program (which RAND refers to as “positive profiling”) could have on the size and cost of EDS installations at large and medium US airports. In a 2004 report, one simulation modeling exercise used the following parameters: size the system to ensure that bags get to the intended flight 99% of the time, assume 90% reliability (uptime) of the EDS machines, and assume that 50% of all bags are exempted from EDS screening (Shaver and Kennedy 2004).

For this set of assumptions, the RAND team estimated the total cost to the flying public of various levels of EDS deployment, where cost includes both the capital and operating costs (screener payroll) of the EDS machines and the extra time currently wasted by passengers getting to the airport early enough to ensure that their flight is not delayed due to slow bag processing. In the absence of a TT program, the optimal number of EDS machines under these assumptions (United States, nationwide) was found to be 6000. But with a TT program that exempted 50% of all bags from EDS screening (defined as screening all bags of non-TT members plus a randomly selected one-sixth of the bags of the 60% of daily passengers who are TT members), the optimal number of EDS machines declines to about 2500. That’s a very large difference in both the space required at airports and also in capital and operating costs. In round numbers, under a reasonable set of assumptions, this kind of TT program could cut costly EDS deployment by up to 50%.

Some of the capital cost savings could be used for any needed expansion of passenger checkpoints and/or for improving terminal access control and airport perimeter control. The latter two uses aim at protecting planes on the ramp from unauthorized persons. And some of the payroll cost savings (from fewer EDS

machines) could be used to add security personnel in lobby areas and to add staff for access control and perimeter control, as necessary.

The risk-based approach should produce significant savings in passenger time, by speeding up baggage screening and passenger screening alike. While the model necessary to quantify such savings is beyond the scope of this paper, the ultimate impact is that people do not have to arrive at airports as early as they have learned to do in the post-9/11 era, reclaiming that time for personal or business purposes.

## 11.5 ALTERNATIVE WAYS OF PROVIDING AIRPORT SECURITY

The provision of airport security varies considerably among countries. All OECD members have designated a single national agency to be responsible for aviation security—Transport Canada in the case of Canada, the TSA in the United States, and usually a transport ministry in European countries. Those agencies are responsible for making *policy decisions* about security (within the constraints of legislative direction) and for *regulating* the various entities involved in aviation—airports, airlines, pilots, and fixed base operators. But which party actually delivers various security functions differs considerably.

Canada is unique in having created a crown corporation responsible for most aviation security functions: passenger and baggage screening, access control, and biometric identity cards. But that organization (CATSA) does not make security policy or regulate airport security. In Europe, security functions are usually the responsibility of each airport. The United States is unique on having a decidedly mixed system, thanks to the way Congress defined the TSA in its 2001 legislation. By law, TSA must carry out passenger and checked baggage screening at nearly 450 commercial airports, despite TSA also being the national aviation policy-maker and regulator. Yet nearly all the remaining airport security functions—access control, perimeter protection, terminal-area policing, etc.—are the responsibility of the airport, under TSA's regulatory oversight.

### 11.5.1 Providing Airport Screening

One of the largest contrasts in providing airport security services is in the use of private security firms for passenger and baggage screening. In countries where the screening function has been devolved from the national policy-maker to either the airport level (Europe) or to a crown corporation (Canada), the most common practice is to outsource screening to government certified security firms.

Europe offers the most decentralized model, with nearly all EU countries having devolved the screening responsibility to the airport level. In most cases, airports are free to hire and manage their own screening staff (meeting national requirements), contract with a certified security firm, or arrange to have screening done by a law enforcement agency. Table 11.1 provides an overview of the screening arrangements at major European airports, as of 2011. Slightly more than half contract with private

**TABLE 11.1** Airport Screening Provision in Europe, 2011

Country	Airports	Screening Provider	Information Source
Albania	Tirana	Contract	ACI, T&I
Austria	Vienna	Self-provide	T&I
Austria	Graz, Innsbruck, Klagenfurt, Linz, Salzberg	Contract	T&I
Belgium	Antwerp, Brussels, Charleroi, Liege, Ostend	Contract	ACI, T&I
Bulgaria	Sofia, Varna	Government	T&I
Croatia	Brac, Dubrovnik	Contract	T&I
Czech Republic	Prague	Self-provide	ACI, T&I
Denmark	Copenhagen	Self-provide	ACI, T&I
Estonia	Tallinn	Contract	ACI, T&I
Finland	Helsinki, Kittila, Oulu, Rovaniemi, Tampere, Turku, Vaasa	Contract	ACI, T&I
France	Paris CDG, Paris Orly, Bordeaux, Lyon, Marseille, Nantes, Nice, Toulouse	Contract	T&I
Germany	Hahn, Frankfurt, Nuremberg, Munich	Self-provide and contract	ACI, T&I
Germany	Berlin, Cologne, Dusseldorf, Hamburg, Hannover, Lubeck, Stuttgart	Contract	T&I
Greece	Athens, Corfu, Rhodes, Thessaloniki, regional airports	Contract	ACI, T&I
Hungary	Budapest	Self-provide	T&I
Iceland	Keflavik	Self-provide	ACI
Ireland	Cork, Dublin, Knock, Shannon	Self-provide	T&I
Italy	Milan, Rome	Self-provide	T&I
Italy	Florence, small airports	Contract	T&I
Latvia	Riga	Self-provide	ACI, T&I
Lithuania	Vilnius	Self-provide	T&I
Malta	Malta	Self-provide and contract	ACI
Netherlands	Amsterdam, Rotterdam	Contract	ACI, T&I
Norway	Bergen, Bodø, Oslo, Trondheim, 42 others	Contract	ACI, T&I
Poland	Cracow, Poznan, Warsaw, 9 others	Government	ACI, T&I

**TABLE 11.1** (*Continued*)

Country	Airports	Screening Provider	Information Source
Portugal	Azores, Faro, Lisbon, Madeira, Porto	Contract	T&I
Romania	Bucharest	Government	T&I
Russia	Moscow—Domodedovo and Sheremetyevo; St. Petersburg	Self-provide	T&I
Serbia	Belgrade	Self-provide	T&I
Slovenia	Ljubljana	Contract	ACI, T&I
Spain	46 AENA airports including Barcelona, Madrid, Malaga, Seville, Valencia	Contract	ACI, T&I
Sweden	Stockholm Arlanda, Bromma, Malmo	Contract	ACI, T&I
Switzerland	Zurich	Government	T&I
Switzerland	Geneva	Self-provide and contract	T&I
United Kingdom	London LHR, London LGW, London STN, Glasgow, Edinburgh, Manchester	Self-provide	T&I
United Kingdom	Doncaster, Durham, Liverpool, London City	Contract	T&I

Sources for the table are two. ACI means Airports Council International—Europe and T&I means Appendix 1 of U.S. House Committee on Transportation & Infrastructure Committee (2011).

security firms, while nearly as many self-provide. Only a handful of airports have their screening services provided by a government agency.

Canada's CATSA was created after 9/11, analogous in some ways to the creation of the TSA in the United States. CATSA was given responsibility for several core functions, including screening passengers and baggage at 89 airports, developing a program for employee access to secure areas of airports, assisting the 17 largest airports financially with the cost of increased policing, developing biometric ID cards for those who need access to secure areas, and coordinating with the Royal Canadian Mounted Police to develop an air marshal program for selected flights. The legislation also changed Transport Canada's security role to that of *policy-making and regulation only*.

For two reasons, CATSA opted to contract with private security providers for airport screening, rather than hiring and training a staff of its own. First, it was under time pressure to get better screening in place at 89 airports. Second, its leaders were aware of the success of outsourced screening in Europe, which dated back to the late 1980s and early 1990s.

In the United States, the situation was more complicated. Prior to 9/11, airport screening was provided by security firms, but they were under contract to the principal airlines at the various terminals of each airport or to the dominant airline at a major hub such as Atlanta or Minneapolis/St Paul. At the national level, airport security was regulated by the FAA. That agency simply required airlines to install metal detectors and simple X-ray scanners for carry-on bags—but provided very minimal standards either for the security firms or the screeners they employed. Screening was viewed by the airlines as an unfunded mandate, and since there were no standards, the airlines all sought to minimize the cost of this mandate, resulting in screeners and screening of generally low quality. The GAO documented this low quality in a series of reports, beginning in 1987, and recommended that FAA set and enforce performance standards, but the FAA failed to act on these recommendations (General Accounting Office 1987).

The White House Commission on Aviation Safety and Security recommended in 1996 that the FAA promulgate licensing and performance standards for screening companies, background checks for screeners, expanded “red team” testing of airport screening, and comprehensive passenger–baggage matching (Armstrong and Pereira 2001). The only recommendation that was put into practice was extending CAPPS from its original airline developer (Northwest) to all other US airlines, though in a restricted form. Congress that year (1996) included in the FAA reauthorization act a requirement that FAA “certify companies providing security screening and improve the training and testing of security screeners through the development of uniform performance standards” (Section 30, Public Law 104-264, 1996). In January 2000, FAA issued a proposed certification rule, but when that rule had not been finalized by November of that year, Congress acted again, requiring issuance of a final rule by May 31, 2001 (Section 3, Public Law 106-528, 2001). But the FAA failed to meet this deadline, so no such standards were in place on September 11, 2001, when the terrorist attacks took place.

The public and many in Congress blamed the private security companies for the hijackers boarding the planes carrying (legal) box cutters—when the actual failure was that the watered-down CAPPS screening failed to flag the hijackers for secondary screening. “Rent-a-guard” screening became the scapegoat, leading to calls for a complete “federal takeover” of airport security. The Senate bill called for exactly creating the TSA that would not only make policy and regulate but also directly provide passenger and baggage screening at 450 airports. The House bill, by contrast, sought to change the form of outsourced screening to follow European practice, which had been documented in a GAO report that year based on site visits to four countries (General Accounting Office 2001). Under the House bill, airports—not airlines—would be responsible for security, and they could do it either with their own staff or by contracting with security firms that had received federal certification. The final compromise legislation created the TSA to do airport screening but allowed an initial five airports to opt out, as a pilot program to test TSA-certified private screening. Several years later, all airports were allowed to opt out on a similar basis.

Performance of the TSA-certified firms at the five pilot program airports (San Francisco, Kansas City, Rochester, Jackson Hole, and Tupelo) has been

evaluated a number of times, by the GAO, by outside consultants hired by TSA, and by the staff of the House Transportation and Infrastructure Committee. They have all found screening performance of the certified security firms to be as good as or better than that of TSA screeners at comparable airports (Bearing Point 2004; Government Accountability Office 2004, 2009). On the question of cost, the early studies showed little difference, given that the legislation required certified contractors to provide employees with the same pay and benefits as TSA screeners. A subsequent study commissioned by TSA but never released was criticized by GAO for a misleading cost comparison that purported to show higher costs for pilot program airports by omitting various TSA costs (Government Accountability Office 2009).

But the 2011 study by the House Transportation and Infrastructure Committee, though comparing only two major airports—TSA-screened Los Angeles International (LAX) and contractor-screened San Francisco International (SFO)—found striking overall differences in cost and throughput (passengers per screener) (U.S. House Committee on Transportation & Infrastructure 2011). The private firm at SFO was far more flexible in its use of employees, successfully using many part-time screeners at peak times without having to pay them for nonbusy off-peak times. It also had a much lower attrition rate; hence, its recruitment and training costs were significantly lower. Attrition at LAX was so high that TSA had to make considerable use of its expensive National Deployment Force—screeners who are flown in and housed in hotels to fill in for vacancies—thereby further increasing the cost of TSA screening at LAX. Overall, contract screening at SFO was found to be 65% more productive, as measured by passengers per screener, than TSA screening at LAX. The study estimated that if the screening at LAX were as productive as that at SFO, its workforce would be 867 persons smaller, saving \$33 million per year.

A better-designed screening outsourcing program would offer considerably more flexibility, by allowing the airports—rather than TSA—to select the screening firm from among those TSA has certified. It could also focus mostly on performance and outcome measures. Today, TSA specifies the exact methods, procedures, and technologies that a contract screening company must use (identical to those used by TSA screeners). A performance-based approach would set measurable outcome goals and allow the company to make use of any TSA-approved technology to achieve them. This would stimulate the market for technology providers to develop a wider array of hardware and software, rather than facing the all-or-nothing odds of being selected as “the” provider of, say, a liquid screening device.

Flexibility is especially important when it comes to matching screener staffing to passenger volume. The deregulated airline industry is dynamic, with new airlines being created, older ones merging or failing, and services being increased or decreased both seasonally and often monthly in response to airline initiatives and the ups and downs of the economy. Numbers of enplaned passengers at US airports fluctuate up and down from 1 month to the next from 10 to 20% for most airports, with some smaller airports experiencing much larger monthly changes (Poole 2006). Yet the TSA’s allocation of screeners to airports is done on an *annual* basis, making it difficult to match staffing to workload. That is the kind of short-term flexibility that outsourcing facilitates.

Another problem that has manifested itself in both Canada and the United States is compensation levels for airport screeners. In both countries, the cost of living and hence pay scales vary considerably from one region to another, with CATSA having some difficulties attracting and retaining screeners in the booming oil province of Alberta. But unlike TSA, CATSA is free to offer different pay scales in different regions.

A larger, long-term advantage of outsourcing was noted in a RAND Corporation paper on how terrorists adapt to defensive technologies (Jackson et al. 2007). Over time, terrorists may learn how to evade the technology or alter their operational practices. Five years from now, a 47,000-person civil service workforce of TSA airport screeners may no longer be appropriate, due either to changes in terrorist methods of operation or to improved technologies. In such a case, it would be far easier to downsize outsourced screening workforces—and redirect the resources to higher-priority uses—than to reduce the number of unionized government employees expecting something akin to lifetime tenure.

Devolution of US airport screening to the airport level would create a potential market for screening companies of well over 400 airports. That large a market would likely draw additional security companies into the field, seeking TSA certification. The market could be even larger if major hub airports with multiple terminals were allowed to select different companies for different terminals. There is a policy question to be debated in this regard, since one of the advantages of getting TSA out of the screening business would be to end the current fragmentation of security responsibilities at the great majority of airports where TSA is responsible for providing passenger and baggage screening and the airport is responsible for all other aspects of security (lobby, tarmac, perimeter). Unified security at an airport, in principle, would be better coordinated, with all functions reporting to and accountable to the airport's security director. There would also be the potential for cross-training of screeners to do other security functions at nonpeak times. Those advantages would be somewhat less if different screening companies operated in different terminals.

Thus, on the question of how airport security functions are provided, the European approach of devolving the responsibility for provision to each airport and permitting outsourcing by airports, under regulatory supervision, seems wisest. It allows for tailoring service levels to local conditions and it offers flexibility to upsize or downsize in response to changing threat levels and numbers of passengers. The least flexible approach is that of the United States, with a highly centralized model and the blurring of regulation and service provision. Canada's somewhat decentralized approach, with outsourcing, is somewhere in between.

## 11.6 PAYING FOR AIRPORT SECURITY

Who should pay for antiterrorism security measures? There is some merit to the argument that international terrorism is a threat to entire societies and that antiterrorism measures are akin to or part of national defense. To the extent that this argument is accepted, airport security and other defenses against terrorism are pure public

goods and should be paid for by all taxpayers. However, if some components of a society present larger and more attractive targets to terrorists, there is some justification for deciding that those who make use of that component should bear some or all of the costs. In this sense, security expenses can be seen as analogous to insurance. In general, in free societies, we allow people to engage in activities with various levels of risk, such as building homes in flood plains or on earthquake faults or building and operating oil refineries. Those activities that are inherently higher risk generally carry higher insurance costs, reflecting those risks. High insurance costs provide incentives for those incurring those costs to take protective measures to minimize risks. In hindsight after 9/11, US airlines learned that their low-performance contracts for passenger screening were inadequate to the task of coping with suicide bomb threats. If the federal government had not taken over that function, it is likely that airlines would have insisted on higher-quality screening services thereafter.

In light of these points, it is instructive to compare how aviation security is paid for in Canada, Europe, and the United States. The Canadian system represents the most transparent case. The Air Travelers Security Charge, enacted along with CATSA, is applied to all airline tickets, with different rates for domestic, transborder to/from the USA, and other international flights. Its proceeds fund 100% of the budget for CATSA, which handles airport security and the funding of air marshals; it also paid the one-time costs of strengthening the cockpit doors of Canadian airliners and pays the costs of additional Transport Canada security inspectors.

Thus, Canadian policy on transportation security appears to be *mode specific*, that is, the costs of protecting a mode of transportation are borne by the users of that mode. (Whether Canada is applying that policy consistently to other transportation modes is beyond the scope of this chapter.) Canadian airport and airline trade associations argue that “aviation security is a ‘national defense’ issue and as such should be funded from general revenues” (Canadian Airports Council 2007). But after making this point, their recommendations (during the 5-year review of CATSA in 2006) all focused on making the present funding mechanism more transparent and responsive to changing needs.

In Europe, the pattern varies by country. In the United Kingdom, the major airports, all of which are commercialized with most now at least partially privatized, are responsible for all airport security, at their own expense. These costs get factored into the cost base on which they charge airlines for airside and landside services. Germany has a federal aviation security tax that is added to airline tickets, but that tax covers only a portion of the capital and operating costs of airport security, the balance of which are paid for out of airport budgets. Some German airports, like Frankfurt, Hamburg, and Dusseldorf, have been part-privatized, while others remain owned by some combination of state (Land) and municipal governments. Thus, in many EU countries, responsibility for aviation security is mode specific, via a mix of passenger taxes and airport costs, with the latter being funded by airline charges. Article 5 of 2008 EC Regulation No. 300/2008 allows for each member state to decide the mix of funding, from the state, airports, airlines, other agencies, and users, presumably passengers and shippers. Thus, Europe is not as mode specific in its approach to security funding as is Canada.

The trend appears to be toward more mode-specific funding over time. A 2009 survey by the European Commission found that 11 member countries rely almost exclusively on aviation fees to support the costs of aviation security, while six sometimes provide significant general tax support for such costs and four did not provide such information (European Commission 2009). The Commission recommended increased transparency to ensure that aviation users can ascertain that such fees are used only for security costs and do not discriminate among airlines or airports. As a step toward that end, it also recommended “one-stop” security for intra-EU passengers—that is, the elimination of rescreening of such passengers when they change planes at an airport within the EU, “provided the infrastructure separates passengers screened under EU requirements from other passengers.”

The United States presents the most complex assortment of funding sources. By 2007, the fraction of TSA’s aviation budget that was provided by security taxes on airlines and passenger tickets slightly exceeded 50%. The balance of TSA’s funding comes from the federal government’s general fund. In addition, airports themselves are responsible for access control and airside security, costs that become part of their cost base and are passed along to airlines via airport rates and charges. Cost estimates for those portions of aviation security expense are not readily available. But because of significant federal general-fund support of TSA’s aviation security budget, the United States departs significantly from the fully mode-specific funding approach of Canada and the increasingly mode-specific funding approach of EU countries. US airlines make the same argument as their counterparts in Canada and Europe: that aviation security is basically a national defense function and should be covered entirely from the federal government’s general fund.

Were US airport security fully funded by the aviation sector, there might be greater resistance by airlines and other stakeholders to excessive TSA costs. For example, a GAO analysis found large differences in the operating costs of baggage screening done via lobby-based EDS machines and so-called in-line screening (in which the EDS machines are installed in the partly automated baggage processing system). In the former, bags must be loaded by hand, whereas in the latter approach, they reach the machine via conveyor belt, in a continuous process. Based on the GAO analysis, Poole estimated the overall labor savings from optimal checked baggage systems at all US commercial airports (Poole 2006). Across the five airport size categories, the number of checked baggage screeners could be reduced by 28%, producing large annual savings in personnel costs.

Another example is TSA’s program to train some of its screeners as behavior detection officers (BDOs), who are supposed to be able to detect signs of stress and nervousness among passengers, justifying the BDO to take the person aside for a brief interview. The GAO did a detailed assessment of this program, concluding that it lacked scientific justification, failed to turn up any would-be terrorists among over 150,000 interviews, and actually failed to spot 16 terrorist suspects who were known to have traveled through eight airports where BDOs were active (Government Accountability Office 2010). Some would challenge this program as typical of agency “mission creep,” but despite its added cost and lack of effectiveness, the US aviation community has failed to challenge it.

If those involved with a particular type of transportation, like the airlines, must bear most or all of the costs of securing that mode against terrorism, they presumably will be more concerned than otherwise about the cost-effectiveness of those protective measures. As the EC report states, “It may be reasonable that security measures are financed, at least in part, by passengers, cargo shippers, and [carriers], as they are best placed to scrutinize the cost implications of security measures” (European Commission 2009). Given the tendency of elected officials to enact grandiose target-hardening plans without benefit of analysis, a countervailing force directly concerned with the costs of those plans seems wise. And airlines to some extent are playing that role of watchdogging costly aviation security measures.

However, the case for mode-specific funding being applied to aviation is only fair (in the sense of not creating distortions in mode choice for customers) if the same principle is applied to the security costs of other transport modes. While an examination of the extent to which this is being done is beyond the scope of this chapter, one indication is provided by a recent US report, from the DHS’s Office of Inspector General (DHS Office of Inspector General 2009). Only in 2005 did the TSA begin to devote resources to surface transportation modes, creating a small workforce of 100 transportation security inspectors (expanded to 175 in 2008). Their initial focus is on mass transit, freight railroads, and passenger railroads. The TSA also operates three surface transportation security grant programs—for mass transit, trucking, and intercity bus transportation. In FY 2008, funding for these three programs totaled \$415 million. While that sum is less than 10% of the TSA budget for aviation, all such funding for surface transportation security comes from federal general funds, rather than from security fees or taxes on the modes in question.

## 11.7 SUMMARY AND CONCLUSIONS

Defending target-rich free societies against terrorism is inherently difficult. On a macrolevel, it seems unlikely that terrorism can be eliminated in a permanent sense; the inherent asymmetries will likely make free societies attractive targets for one or another terrorist group indefinitely. We also know that terrorists learn from experience and can change tactics and targets in response to defensive measures. Therefore, defensive measures must be dynamic and flexible, rather than static and predictable.

Most of the current aviation security policies and programs in Canada, the EU, and the United States are responses to previous terrorist attacks, rather than more broadly based protections against a range of possible future threats. It seems likely that a number of such programs (e.g., air marshals, body scanners, and 100% EDS screening of checked baggage and belly cargo) would not pass a test of relative cost-effectiveness, such as the annual cost per life saved. Yet risk assessment, though much talked about as providing a sound basis for setting security priorities and allocating resources, seems to be very difficult to put into practice, despite its potential for getting significantly more value from the always limited amount of resources available in a country for aviation security.

In the United States, the largest resource allocation decisions have been made not by the designated security agency, the TSA, but by the US Congress and enacted as legislation. These include the mandates for 100% EDS screening of checked baggage and 100% physical screening of belly cargo, the creation of TSA with the dual roles of aviation security regulator and airport screening provider, and a static, “fortress wall” approach to airport screening. These decisions were not based on analysis by security experts, but rather by elected officials seeking to reassure the public that aviation is well protected, regardless of cost or secondary effects.

One possible incentive for a more risk-based policy is mode-specific security funding—for example, that the costs of aviation security be paid for by aviation system users. This gives that user group an incentive to monitor the costs and cost-effectiveness of security programs that affect it, serving to some extent as a counter-weight to politicians’ tendencies to impose costly but ineffective programs. In this regard, Canada most closely adheres to this principle, with the United States departing the most from it and Europe in between.

In terms of flexibility, the EU countries have devolved airport security functions most completely to the airport level (under national government regulatory supervision), permitting resources to be tailored to need and, thanks to outsourcing, permitting changes in workforce levels in response to changing threat and demand levels. Canada makes wide use of outsourcing but in a more centralized model that does take account of regional cost differences. The United States is least flexible, with all passenger and baggage screeners (except for a handful employed by highly regulated contract firms) working directly for the federal government. In addition, the US model results in fragmented security responsibility at the airport level, with the TSA providing screening services and the airport providing all other security functions.

Rhetoric in all the countries examined here supports risk-based security, and indeed, that is largely the practice in all forms of goods movement, including air cargo. Perhaps that is because cargo is much less visible to the public and because the consequences for supply chains would be so great if passenger-type security measures were applied to all goods movement. The GAO’s expert panel on strengthening the use of risk management principles was asked to identify the “key challenges” to doing so (Government Accountability Office 2008). The number one challenge (35% of panelists) was to “Educate the public about risks and engage in public discourse to reach consensus on an acceptable level of risk.” Number two (19%) was to “Educate policymakers and establish a common lexicon for discussing risk,” to counteract political obstacles to risk-based resource allocation.

The goal of such efforts should be to wean legislators away from enacting mandates not based on risk analysis. Legislators should be encouraged to direct the national aviation security policy-maker/regulator to address various problems within some kinds of quantitative parameters (e.g., the US DOT’s \$3 million per life saved measure). Details of making actual policy and resource allocation decisions should be left to the aviation security agency. That agency, in turn, should be flexible in tailoring policies to changing threats and different situations at individual airports, which vary enormously in type, size, configuration, etc.

No security policy should be pursued “at all costs,” since resources are always limited. Likewise, all possible targets cannot be hardened to any appreciable degree, without bankrupting a country. While it seems likely that commercial aviation will remain a high-profile potential target, spending billions every year on static defenses at airports is almost certainly a poor use of resources. Whether any kind of effort can succeed in educating elected legislators and opinion leaders to these realities is the most difficult challenge.

## REFERENCES

- Advisory Panel (2006) Flight plan: managing the risks in aviation security: review of the Canadian Air Transport Security Authority Act ([www.gazette.gc.ca/rp-pr/p1/2014-11-01/html/reg1-eng.php#footnoteRef.47255](http://www.gazette.gc.ca/rp-pr/p1/2014-11-01/html/reg1-eng.php#footnoteRef.47255)), accessed February 18, 2015.
- Airports Council International-Europe (2006) Airports and airlines launch joint action to tackle aviation security. News release, October 10.
- American Association of Airport Executives (n.d.) AAAE and the transportation security clearinghouse ([www.aaae.org/federal\\_affairs/transportation\\_security\\_policy/tsc.cfm](http://www.aaae.org/federal_affairs/transportation_security_policy/tsc.cfm)), accessed November 10, 2008.
- Armstrong, D and Pereira, J (2001) Nation’s airlines adopt aggressive measures for passenger profiling. *Wall Street Journal*, October 23.
- Auditor General of Canada (2005) National security in Canada: the 2001 anti-terrorism initiative: air transportation security, maritime security, and emergency preparedness ([www.oag-bvg.gc.ca/internet/English/parl\\_oag\\_200504\\_02\\_e\\_14933.html](http://www.oag-bvg.gc.ca/internet/English/parl_oag_200504_02_e_14933.html)), accessed April 15, 2015.
- BearingPoint (2004) Private screening operations performance evaluation report. Transportation Security Administration, April 16.
- Business Travel News* (2008) One-on-one: TSA Administrator Kip Hawley preps his final initiatives. October 20.
- Canadian Airports Council (2007) CATSA act 5-year review: CAC position paper.
- Davis, A, et al. (2002) Security concerns bring focus on translating body language. *Wall Street Journal*, August 15.
- DHS Office of Inspector General (2009) Effectiveness of TSA’s surface transportation security inspector. OIG-09-24, February.
- European Commission (2009) Report from the Commission on Financing Aviation Security. COM (2009) 30, February 2.
- Foster, C, et al. (2003) *Enhancing aviation security with the SWIFT system*. H. John Heinz III School of Public Policy and Management, Carnegie Mellon University, Pittsburgh, PA, May 18.
- General Accounting Office (1987) Aviation security: FAA needs preboard passenger screening performance standards. GAO-RCED-87-182, July 24.
- General Accounting Office (2001) *Aviation security: terrorist acts demonstrate urgent need to improve security at the nation’s airports*. Testimony of Gerald Dillingham, Senate Commerce, Science, and Transportation Committee, Washington, DC, September 20.

- Government Accountability Office (2004) Aviation security: private screening contractors have little flexibility to implement innovative approaches. Testimony of Norman J. Rabkin, GAO-04-505T, April 22.
- Government Accountability Office (2007) Department of Homeland Security: progress report on implementation of mission and management functions. GAO-07-454, August.
- Government Accountability Office (2008) Risk management: strengthening the use of risk management principles in homeland security. GAO-08-904T, June 25.
- Government Accountability Office (2009) Aviation security: TSA's cost and performance study of private-sector airport screening. Briefing for congressional requesters, GAO-09-27R, January 9.
- Government Accountability Office (2010) Aviation security: efforts to validate TSA's passenger screening behavior detection program underway, but opportunity exists to strengthen validation and address operational challenges. GAO-10-763, May.
- Homeland Security* (2007, August) Issue 6.
- International Civil Aviation Organization (ICAO) (2006) Security: safeguarding international civil aviation against acts of unlawful interference. Annex 17, eighth edition, ICAO.
- International Transport Forum (2009) *Round table on 'security, risk perception, and cost-benefit analysis,' Paris, summary and conclusions*. Round Table 144. OECD International Transport Forum, Paris.
- Intriligator, M (2008) *On 'transnational terrorism' – perspective paper on the Todd Sandler, Daniel G. Arce, and Walter Enders paper for the 2008 Copenhagen Consensus*. Copenhagen Consensus Center, Copenhagen.
- Jackson, B et al. (2007) Breaching the Fortress wall: understanding terrorist efforts to overcome defensive technologies. RAND Corporation ([www.rand.org/pubs/monographs/2007/RAND-MG481.pdf](http://www.rand.org/pubs/monographs/2007/RAND-MG481.pdf)), accessed February 18, 2015.
- Levine, M and Golaszewski, R (2001) E-ZPass for aviation. *Airport Magazine*, November/December.
- Lo, C (2013) Securing IATA's checkpoint of the future. *Airport Technology*, February 8.
- Morral, R et al. (2012) *Modeling terrorism risk to the air transportation system*. RAND Homeland Security and Defense Center: Santa Monica, CA.
- Oster, C and Strong, J (2008) A review of Transportation Security Administration funding, 2001–2007. *Journal of Transportation Security*, 1: 37–43.
- Poole, R (2006) *Airport security: time for a new model*. Policy Study No. 340, Reason Foundation (<http://reason.org/news/show/airport-security>), accessed February 18, 2015.
- Poole, R (2009) Towards a risk-based aviation security policy. In: *Terrorism and international transport: towards risk-based security policy, round table 144*. OECD International Transport Forum: Paris.
- Regulation (EC) No. 300 (2008) of the European Parliament and of the Council, of 11 March 2008 on Common rules in the Field of Civil Aviation Security (and repealing Regulation (EC) No. 2320/2002).
- Sandler, T. et al. (2008) *Terrorism: Copenhagen consensus 2008 challenge paper*. Copenhagen Consensus Center: Copenhagen.
- Shaver, R and Kennedy, M (2004) The benefits of positive passenger profiling on baggage screening requirements. DB-411-RC. Rand Corporation ([www.rand.org/pubs/document\\_briefings/2004/RAND\\_DB411.pdf](http://www.rand.org/pubs/document_briefings/2004/RAND_DB411.pdf)), accessed February 18, 2015.

- Stewart, M and Mueller, J (2008) A risk and cost-benefit assessment of United States aviation security measures. *Journal of Transportation Security*, 1 (3): 143–159.
- Stewart, M and Mueller, J (2011) Cost-benefit analysis of advanced imaging technology full body scanners for airline passenger security screening. *Journal of Homeland Security and Emergency Management*, 8 (11).
- Stewart, M and Mueller, J (2013) Terrorism risks and cost-benefit analysis of aviation security. *Risk Analysis*, 33 (5): 893–908.
- U.S. House Committee on Transportation & Infrastructure (2011) TSA ignores more cost-effective screening model,” June 3 ([http://archives.republicans.transportation.house.gov/Media/file/112th/Aviation/2011-06-03-TSA\\_SPP\\_Report.pdf](http://archives.republicans.transportation.house.gov/Media/file/112th/Aviation/2011-06-03-TSA_SPP_Report.pdf)), accessed February 18, 2015.



---

# 12

---

## SEAPORT OPERATIONS AND SECURITY

WILLARD PRICE AND ALI HASHEMI\*

*Eberhardt School of Business, University of the Pacific, Stockton, CA, USA*

### 12.1 SEAPORTS IN THE GLOBAL SUPPLY CHAIN

One dominant cause of globalization is the invention, in the early 1960s, of the shipping container. This container, affectionately known as the “box,” is a closable storage device easily moved on and off oceangoing vessels. After loaded or stuffed by the originator, it is then delivered to shipping companies and distributed to the recipient by logistics services (Levinson 2006). The box made loading and unloading cargo much cheaper, eliminating the traditional cargo net and longshoremen at seaports, so necessary when products were moved by themselves or in smaller packages or cases. Globalization would not have its strength without the container and compatible logistics.

Trade is stimulated by global trade agreements, both multilateral and bilateral, with the goal to ease barriers to trade, prohibit or minimize tariffs, and lessen the challenge of regulatory hurdles. Further open borders between trading states are expected by the World Trade Organization (WTO) and emerging agreements such as the Transpacific Partnership (TPP) and a new United States (US)–European Union (EU) compact. Trade agreements demand less complexity at the border crossing, yet the free flow of goods, in containers, can include desirable and possibly undesirable (or nefarious) goods.

\* Research assistance.

### 12.1.1 Seaport Security and Terror

An effective security strategy against the entry of terrorists and dangerous materials must be present if ports or terminals are to avoid the risk of harm to the United States (US). As the terror threat became real with the 9/11 attacks, ports were assumed to be a target or avenue for terror. Shipping containers would serve as a useful conduit for terrorists and their weapons, yet full inspection or opening of all sealed shipping containers at the terminal was not acceptable to anyone. Such delay would create chaos in cargo movement through the port and would require large numbers of inspectors, be they port or federal employees.

Nonetheless, the threat to seaports and the hinterland from terror attacks, as well as the limited ability of the nation to prevent such attacks, should be heard. This security challenge is well chronicled in two books by Stephen Flynn (Flynn 2004, 2007). In a 2005 article, Flynn provided an interesting analogy on port security, a statement, still quoted in a 2013 *Time* article by Fareed Zakaria:

The US Navy invests more in protecting the single port of San Diego, home to the Pacific Fleet, than Department of Homeland Security (DHS) has invested in the ports of Los Angeles, Long Beach, San Francisco, Oakland, Seattle and Tacoma combined. (Flynn 2005; Zakaria 2013)

This chapter seeks to inform the conversation about port operations and security initiatives by describing port infrastructure, providing an analysis of terror risk that defends a security barrier, evaluating the contribution of security technology for cargo scanning or non-intrusively see within shipping containers and presenting the debate on the extent of such container inspection. Responsibilities among governments and private port operators for developing and funding security initiatives are contrasted, and, finally, the chapter is summarized by a research agenda to address unresolved questions in port security.

## 12.2 SEAPORT INFRASTRUCTURE

Supply chains are a network of nodes and modes. Nodes represent locations in the chain where materials or cargoes may dwell as they are shifted between modes of transportation and consolidated or distributed for further shipment. Seaports are significant nodes in supply chain flows since so many goods are shipped via ocean ships able to carry volume and weight and generate lower unit costs. Seaport cargoes involve liquid bulk, dry bulk, and neo bulk (open materials), with the dominant cargo volume and value now in omnipresent closed shipping container. Containers, the principal focus of this chapter, are the prized cargo of many seaports, generating a large share of revenues for shipping companies, terminal operators, and public-private seaport authorities. Container operations at the Port of Los Angeles are shown here (Fig. 12.1).



**FIGURE 12.1** Maersk container ship.

Seaports require a harbor with depth, piers, and alongside space; covered buildings and open storage; paths connecting transportation corridors; mobile vehicles and equipment; and, increasingly, security infrastructure with physical barriers, detection equipment, and inspection technology. Information systems must record, store, and report terminal/shipment performance in real time and be available online.

### **12.2.1 Port Capability/Capacity: Terminal Performance**

Fixed and movable infrastructure is developed, with public port owners conducting design, construction, and operations, often choosing to use consultants/contractors or engage in public–private partnerships. Private sector actors may also invest in port infrastructure, dominating most port operations. Yet a current question is whether these logistics operators are obligated to invest and conduct security operations.

To serve the demand, seaports require infrastructure with adequate capability and capacity:

Capability: Equipment is obviously needed to handle expected cargo size and weight with adequate speed, reliability, and productivity.

Capacity: Sufficient land and facilities for timely cargo movement, minimum dwell, and flexible resources to serve demand surges allow ports to be competitive.

Ultimately, ports compete on the basis of terminal or shipment performance:

Traditionally: Ports have to produce accurate shipments, flexible responses, operational safety, and secure cargo from thieves. They must perform without delay or wasted costs while creating cargo productivity improvement to allow stable or declining fees.

Currently: Terminals transfer cargo with an added burden to secure port access and prevent terror events. They require shipping container inspection for undesirable materials and persons, securing infrastructure and cargo while minimizing damage and disruption.

### 12.2.2 Seaport Border and Terror

Besides serving as a logistics terminal, seaports act as a border crossing, where cargo originating in one nation seeks to debark in another. It is expected terror events are planned outside the United States and need to enter the port to deliver their terror, whether harm is intended at the port or across the country. The customs process addresses cargo transiting national borders and is operated by the US federal government. After 9/11, customs is now the burden of the Department of Homeland Security (DHS) and its Coast Guard, Bureau of Customs and Border Protection (CBP), and Immigration and Customs Enforcement (ICE).

Terrorists may act to pass through the seaport, with or without materials, to do damage elsewhere, or they may seek to disrupt cargo, destroy property, harm people, and encumber economic activity at the port. Today, the arrival of terror, with the inclusion of nefarious materials in closed shipping containers, demands more sophisticated inspection to assure security and prevent consequences. Terror events can include explosives, rockets, grenades, or weapons of mass destruction impacting terminals, vessels, storage spaces, piers, quays, shipping channels, cargo, and people at the port or inland.

Yet nuclear material emitting radiation is the most feared substance from terrorists. Today, these materials are identified as Radiological Dispersal Devices (RDD), actually weapons of “mass disruption” rather than weapons of mass destruction (RPM 2013). Nuclear materials can be shielded in a container and are most difficult to detect when entering port. The technology critique in the following text describes Radiation Portal Monitors (RPM) and their role in cargo scanning.

Terror can be delivered by container, small boat, weapons launch, and suicidal terrorists. Besides destroying all or part of the port, terror attacks can drop a bridge or sink a vessel in a harbor channel, in effect stopping ships from entering or exiting the harbor. Terrorists seek national symbols for damage, attempt to kill or injure many citizens, and cause economic disruption for the port, state, and national government. They hope to cause trauma and create property, human, and financial disaster for any national target. Terror groups likely have no direct complaint with the

port or even the shipping company, yet seaports are well-known public infrastructure and a readily available economic target with a perceived porous border.

### 12.3 SEAPORT SECURITY STRATEGY

For the most part, port development in the United States occurs within public seaports under the authority of local or state governments, often financially independent public enterprises. Historically, the federal government has minimally invested in ports, serving dredging and other economic development purposes. In the case of national security, federal agencies are expected to fund desired security initiatives and technology and to conduct security operations through DHS. Supply chain actors, including seaports, do not believe they cause or should be responsible for terror. Rather, national policies create terrorists and the broader public often feels the impacts of terror disruption and destruction. Given this national interest, federal policy has been willing to fund port security infrastructure. Whether these national investments are sufficient to avoid disaster from terror events is not yet proven because security strategy is still in development and security methods and decisions remain in debate. Terror is also a risk for logistics carriers who send and receive cargo. Supply chain participants cannot avoid some responsibility for infrastructure and security initiatives, since these partners are actively involved in cargo movement and are also the target of terror events. Surely, it is in their interest to deter terrorists from affecting their facilities, equipment, and cargo.

Terror has a life cycle that includes planning, financing, recruiting, and conducting a terror event, with the hope of a “getaway” and return to obscurity by those who plan and conduct terror. Any attempt to prevent or mitigate terror must decide where to intervene to have the most influence in avoiding disaster. While the port and its partners are involved, it is inevitable that the federal government leads with substantial security initiatives, deciding how to balance its resources between prevention and response actions. Prevention seems so desirable to eliminate disastrous consequences, but it may be difficult to imagine prevention strategies that truly protect ports, cargo, and the nation. Required investments must gain political support while they may be resisted. For this author, it appears all too often response and recovery trump prevention as seen in the many disasters the nation fails to avoid. No doubt there is an honest attempt by seaport security to prevent terror success by disrupting terrorist plans and creating physical and technology barriers at seaports.

Ports, operators, shippers, and customers more easily support enhanced security that the federal establishment approves and funds. The federal goal is to minimize port vulnerability so as to protect the national interest, but it is not clear that seaports and supply chain partners would act on their own to fully resist terror. Those who determine the probability of a successful attack to be small may take the risk of disaster and not threaten their financial margins.

### 12.3.1 Terror Success or Failure

There has been much debate about prevention, even substantial action, but across the globe, terror does succeed. Here are two examples of terror success through seaports:

On October 12, 2000, the USS Cole was attacked in the Port of Aden harbor, Yemen, by a small boat with explosives, not detected or resisted, even by the US Navy.

On November 26, 2008, terrorists entered the seaport, preceded to destroy hotels in Mumbai, India, without detection or prevention in the harbor or the city.

These successes occurred because barriers and security forces were unable to prevent access in or through the port. There likely are instances in which terror was avoided by prevention strategies, and if these cases can be identified, valuable lessons can be learned. Although very difficult to determine the share of terror failure, a few shipping containers across the globe have been discovered with terrorists and/or dangerous materials and intercepted before damage was done. A few well-known terrorist efforts have been prevented at roadway borders or in airplanes. This prevention achievement, together with limited evidence of terror success, minimizes attention to prevention efforts at seaports.

Many governments and logistics operators still expect ports to be a preferred target for terror events as the examples earlier demonstrate. A seaport is often viewed as a porous border because terrorists can enter the country via ship or container with less chance of customs, border patrol agents, and port security forces discovering and apprehending those who aspire to do harm. The US Congress and DHS have devoted significant resources to decrease the vulnerability of ports as they have conducted at airports and land border crossings. It must be assumed that terror groups are constantly imagining new terror events at seaports, even though they may not know the specific port vulnerability. Do DHS and the ports themselves know the probability of a threat to their vulnerability?

### 12.3.2 Knowing and Avoiding Risk

The risk or uncertainty that a port or its operators face is a relatively simple joint probability calculation if actual probability distributions can be accurately known. One representation is adapted from Yacov Haimes's prescription for this risk (Haimes 2002):

$$\begin{aligned} \text{Terror risk} = & \text{probability of an attack (threat)} \times \\ & \text{probability of access to port (vulnerability)} \times \\ & \text{consequences of the terror attack (impact)} \end{aligned}$$

Not enough is known about the threat of terror and the impact of any event to confidently estimate the expected impact of losses from a successful event. An annual expected loss could be calculated and compared to the annualized cost of prevention. Security investments may not be accepted if the expected impacts saved by prevention do not exceed the prevention expense.

There is a “curtain of mystery” where governments and others who may know more about terror plans and possibilities intend to keep the curtain closed for fear of aiding the enemy (Price 2004, 334). While this curtain may deny information to terrorists who could refocus their plans if vulnerabilities were known, the bigger question is whether decision makers preparing prevention strategies for seaports have adequate statistical information to actually conduct the decision analysis and benefit/cost calculation suggested previously.

The rigor of decision theory would say port security actually involves “uncertainty and not risk” given the absence of confident knowledge on the probability distribution of terror outcomes. If security professionals and port participants find it near impossible to identify the measured risk of terror success, then it is difficult to say what they are willing to absorb or prevent. Although port operators appear to accept the risk because they view terror events as relatively unlikely, a successful attack can cause catastrophic outcomes. So why do governments, ports, and private operators accept this likelihood if a “risk-avoiding” strategy is available?

There are so many recent cases of public and private organizations willing to neglect effective prevention, coldly accepting the response burden. Well-known cases demonstrate a failure to avoid risk because “prevention is ignored, decided illogically, inadequately funded or considered irrational.” Such strategies imply that disastrous consequences are acceptable. Massive deaths and destruction resulting from a port disaster should be sufficient to justify an attempt to provide a full and effective barrier against terror at a maritime harbor. Both governments and private logistics operators must explain their preferences for prevention, but private sector partners are more able to take a risk and avoid investments in security. They rely on Federal support for prevention and/or federal/state subsidy and insurance for response to terror events.

Even though a major terror action has not occurred at a US seaport, there are enough instances of terror globally to recognize the risk. History tells us to continually strive to out-imagine terrorists if DHS and public ports want to avoid the humiliation of a terror strike. A comprehensive and effective security system is expected, requiring a complete and credible barrier.

### **12.3.3 Security Barriers at Seaports**

A physical system creating the required barrier includes security infrastructure and equipment and human interaction. This security system must be confirmed as complete and effective, eliminating any vulnerability for the port:

1. Fences, road barricades, and gates must prohibit entry of individuals or cargo that is hazardous to the port or nation. Yet they must allow traffic of trucks or trains to pass, so the question is whether cargo, particularly closed containers, need inspection before allowed to enter or leave the port.
2. Bioidentification of workers in the port or operators of trucks/trains will deter unwanted entry. The system currently employed by the DHS is the Transportation Worker Identification Credential (TWIC) where an electronic identification intends to minimize inappropriate entry (Boske 2006, 34).

3. Vehicles and cargo containers must display bar codes for optical character readers (OCR) or use radio frequency identification (RFID) devices to allow immediate identification of the shipper and cargo. These technologies are necessary to more easily track and quickly find any particular shipment.
4. Mobile security forces allow humans to further identify people or cargo not allowed or attempting to avoid the barriers and inspections. Humans have high flexibility and can fill the void if terrorists find a way to beat the technology. Since human patrols are often limited, random patrols hope to close this security gap and certainly can respond quickly to recognition of suspect individuals or cargo. A waterside patrol boat is seen in a picture later near a ship at the Port of Stockton, California, prepared to interdict an attack from the harbor (Fig. 12.2).
5. The greatest challenge to security is the passage of closed container cargo through the port that, reluctantly, must be noninvasively scanned to detect nuclear, biological, and chemical materials or weapons capable of havoc in the port or elsewhere in the country. Container inspection is the main battleground in the security battle and a critical part of the barrier between terrorist and defender.

Most suggest that nuclear material, capable of emitting radiation, is the main threat at seaports. This material can be shielded so a barrier is only ensured if scanning technology can recognize the shape and density of the shield and determine the presence of the nuclear material by separate inspection using a nuclear safe method.

Human contribution is needed at every stage of security, making crucial decisions on when to intervene in cargo transfer and capable of apprehending terrorists or



**FIGURE 12.2** Port security boat.

vehicles. Technology adds efficiency and possibly accuracy to security operations, but technology and humans counter each other's weaknesses to ensure effectiveness. Interpretation of screen displays and data scans as well as decisions for further inspection often require human evaluation—albeit humans are more creative in unusual conditions where machines still have limited capability, even though repetitive actions by humans can cause more errors and certainty higher costs. The balance within the human-machine interface is evolving, and eventually, more autonomous technology will be available that can sense, interpret, and react as being demonstrated in current military and law enforcement robotic applications. An elaborate critique of seaport security technology follows, demonstrating several issues remaining in the implementation of scanning equipment.

## 12.4 SECURITY TECHNOLOGY

Scanning technology or “nonintrusive” inspection has received extensive basic and applied research. The Lawrence Livermore National Laboratory (LLNL), supported by the US Energy and Defense Departments, has been active in developing passive and active scanning or detection technology, addressing nuclear material and chemical and biological substances that can invoke mass destruction (Meissner 2010). The LLNL technology along with other researchers has stimulated development of scanning portals along cargo paths from pier to exit, including a “smart buoy” that can scan ships for a nuclear signature as they enter the harbor (Price 2007, 571). Private security firms have developed equipment to investigate containers at stationary portals on road or rail paths or by mobile portals, moving to cargo that demand inspection. The pictures of both types of portals were taken at Maersk’s Terminal 400 at the Port of Los Angeles (Figs. 12.3 and 12.4).



**FIGURE 12.3** Fixed security portal.



**FIGURE 12.4** Movable security portal.

There are several vendors around the globe designing and delivering scanning technology to serve the expected large market for scanning devices. A graduate thesis from Rotterdam by Miguel Fernandez identified major security vendors across the globe bringing competition to inspection markets (Fernandez 2009). In Europe, the leading vendor is Smiths Detection; in China, it is Nuctech; and in the United States, the companies are Science Applications International Corporation (SAIC) and Rapiscan.

A comprehensive analysis of seaport security vendors would be useful to acquisition decisions but also important as technology evolves and scanning experience is gained. The technology functionality, reliability, and effectiveness offered by each vendor should be available for the buyer, be it DOD, DHS, or transportation/logistics providers. Decisions makers acquiring technology need to know the credibility of their security investments (Price 2007, 571–572).

#### **12.4.1 A Technology Vendor**

While any researcher should be cautious in appearing to favor a particular company's technology without a thorough comparison, this section will critique technology offered by one company actively involved in designing and developing scanning technology: SAIC. Developers and users of security equipment may be hesitant to reveal extensive specifics on the technology's performance, possibly because such secrecy shields weakness in these systems or because too much public detail aids terrorism. Yet SAIC provides significant information to inform those considering their technology.

First, the main functionality of SAIC's seaport security products is highlighted from their webpage with information offered on their technology's false alarm rate as well as the equipment's effect on cargo flow (SAIC 2013):

1. *AT 580 Radiation Portal Monitor (RPM)* is a fixed radiation scanning portal detecting and locating radioactive materials in trucks, containers and railcars; scanning vehicles in the typical flow of checkpoint traffic without requiring vehicles to stop or occupants to exit; false alarm rate better than 1:10,000; operator friendly, humans sound the alarm.
2. *ST 20 RPM* is a fixed spectroscope RPM detecting, locating and identifying radiation material in trucks, containers or railcars; operates in the normal flow of traffic with high throughput; operator software provides alarms, displays, radiation measures and vehicle images, in an integrated system database; false alarm rate as above.
3. *IR 6500 VACIS (Vehicle and Cargo Inspection System) Railcar Portal* is a solution for inspecting railcars and cargo containers on rail in high volume operations; integrates three scans: x-ray imaging, radiation detection and RF identification (RFID); scans an entire train without stopping while delivering a high throughput and small footprint.
4. *Portal VACIS Full Scan Vehicle Imaging System* non-intrusively scans vehicles and cargo, capturing content of vehicles in either “stop and go mode” or “container mode” driving without stopping; allows a typical flow of checkpoint traffic while providing images.
5. *Mobile VACIS Imaging System* is mounted on a rugged truck chassis, allowing trained operators to see contents of closed vehicles and containers while verifying shipping manifests; mobile unit moves past stationary unoccupied vehicles with a quick scan or operates in stationary mode with a high number of trucks moving through inspection under their own power.

Another set of significant concepts is captured from a paper presented by SAIC (Orphan et al. 2009). The value of their presentation is the deliberate focus on four necessary concepts to understand container inspection: integrated container scanning, cargo productivity, shielded radioactive sources, and, most interestingly, the human-machine interface in the risk-based nonintrusive inspection (NII) methodology.

1. *Integrated scanning:* SAIC titles their portal an “Integrated Container Inspection System (ICIS), comprised of a vehicle and cargo inspection system (VACIS), radiation portal machine (RPM) and automated container identification using optical character reading (OCR) devices, enhancing the ability to detect nuclear or radiological material. Three separate container scans can be integrated in location and by interpretation.”
2. *Cargo productivity:* SAIC defends their ICIS suggesting “the primary inspection method included is a passive gamma ray and neutron detection equipment permitting recognition of threat level radioactivity at practical speeds up to 30 km/h to avoid impacting cargo throughput.”
3. *Shielded radioactive source:* SAIC argues, “If the radioactive source is heavily shielded by dense, ‘high Z’ material, passive detection technique may fail to detect the source. A complementary technique such as X-ray or gamma ray

radiograph can detect this dense material. A human viewing the image can spark a secondary inspection with a handheld isotope ID system to verify container contents. Imaging can also verify contents as consistent with the manifest, helping to avoid Type I error alarms from naturally radioactive material.”

4. *Human-machine interface:* SAIC accepts the need for a human-machine by an “andon light” analogy the technology generates on the ICIS viewer screen:
  - a. A green indicator on the screen tells viewers that the automatic algorithm has made a decision to pass the container without further review.
  - b. A yellow indicator suggests a portion of the container cannot be interpreted and human operator must intervene and decide to inspect as necessary.
  - c. A red indicator tells the human reviewer that the automatic algorithm determines the container must be taken aside and opened for inspection.

Like so many current uses of production, logistics, or inspection technology, enhanced automation is likely coming that can sense, interpret, and act autonomously. In the meantime, possibly forever, technology choices will require human intervention when automation is unable and/or the user is unwilling to let the machine act on its own. Researchers in seaport security should observe this trade-off between the autonomy of machines and people in global logistics.

Overall, this critique concludes scanning technology vendors can deliver functionality and availability, at a cost acceptable to security planners. Yet it is not determined here which ports have committed to which vendors for scanning portals. Ports may have hesitated to implement security technology because they believe existing security is adequate, enhanced security systems cannot be justified, or they are waiting for federal grants to support investments. Yet any decision maker should determine the effectiveness and productivity of scanning technology before committing capital. A summary of scanning technology’s performance follows.

#### 12.4.2 Technology Performance

The thesis from the Netherlands referenced earlier had another purpose—to study productivity impacts of these technologies and create understanding of waiting and economic costs of security. Fernandez’ (2009) research presents a model to judge the impact of several configurations of container inspection, concluding the best configuration is to scan at all gates (trucks and trains) as well as transshipment movements ( barges and ship to ship) via the present integrated security system (ISS) accepted by the various federal programs.

One key factor in the scanning debate is the time spent imaging cargo, detecting nuclear radiation, and observing the manifest of the contents, in essence the extra time consumed by inspection. Time delays relate to additional costs for shippers, transporters, and customers with slower cargo movement, so the question is whether screening is swift enough for the ports. A SAIC representative states their most recent scanning design offers high throughput in the normal flow of traffic at gates

or checkpoints—at a rate of at least 150 containers per hour (Rockwood B., Email communication between Willard Price and SAIC's Bryan Rockwood, December 2012). More data on scanning delay needs to be gathered, particularly since logistics operators use this variable to resist container inspection.

The performance of security technology is primarily judged by these two measurements:

Effectiveness: Share of false positive and proportion of false negative results or Type I and Type II errors

Productivity: Time required to conduct inspection or the flow rate measured as containers per hour during scanning

In addition, an evaluation of technology needs two more measurements:

Reliability: Probability of equipment breakdown (fail or crash) frequency and the resulting downtime

Fixed/variable costs: Decisions still need to justify security investments by completing a capital/operating cost analysis

A complete understanding of security systems allows these design choices:

1. Functionality requires the ability to gather information nonintrusively from three scans: images of contents showing shapes and densities, radiation detection, and optically read manifest data. Some combination of human and/or machine interpretation and autonomy must be selected.
2. Scanning systems accuracy must be acceptable for both Type I errors, where the inspection suggests an intervention or opening of the container when the contents are actually not a threat, causing waste but not serious consequences, and Type II errors, where cargo is released when it is actually a threat. This latter condition is unknown until the terror event occurs. A design strategy should reduce both Type I and Type II errors.
3. Ports certainly demand high flow rates through scanning technology, even as traffic is slowed at a checkpoint or gate. Scanning equipment located in the most direct path minimizes time through the terminal. All containers can be scanned, as cargo is unloaded, at a mode transfer stage or at the exit gate. If less than all containers are scanned, a diverted path for inspected cargo seems preferable.

Most technologies are expected to improve over time and design opportunities will be expanded, improving productivity and effectiveness. Design decisions will be influenced by those responsible for developing and funding scanning systems and competing forces among government security offices, logistics operators, and seaport managers. Battles will occur over security obligations involving traditional intergovernmental and public-private trade-offs.

## 12.5 SECURITY RESPONSIBILITY

Supply chain customers and operators across the globe—originators, consignees, freight forwarders, transportation carriers, terminal operators, port authorities, state and local seaport owners, and the prime target for terror, the US government—are potential victims of security weakness. To address terror at its origin, only federal agencies can gather intelligence, identify terrorists, disrupt terror networks, and apprehend individuals planning events before they arrive at a port. Yet such strategies are not likely to stop all attacks. Seaport barriers, screening of ships and vehicles, and cargo inspection are needed to prevent entry of unwanted people and dangerous materials. At this time, the primary security responsibility rests with federal plans and resources.

### 12.5.1 Federal Commitment

If the US government continues to accept responsibility to prevent and detect terror through global surveillance and port inspection, they are required to plan and fund security infrastructure and technologies. The DHS has developed several initiatives and statutes since 9/11 and the birth of the War on Terror. Driven by statutes and regulations, ports, carriers, and operators must cope with these federal requirements:

1. Maritime Transportation Security Act (MTSA) and Operation Safe Commerce (OSC) are early programs passed shortly after 9/11 to develop and test security strategies, providing guidance and grants to support security measures at seaports as well as to solicit participation in prevention by supply chain actors at foreign and domestic ports (World Shipping Council 2012).
2. Automated Targeting System (ATS), a computerized decision support system, reviews documentation submitted by ocean carriers on cargo destined for the United States to help identify shipments requiring additional scrutiny. ATS uses mathematical models with weighted rules to assign a risk score to each shipment (US GAO 2008).
3. Container Security Initiative (CSI) demands information to identify container manifests 24 hours in advance of embarkation at foreign and US ports to determine the security needs before the cargo passes through the port (Haveman et al. 2007).
4. Customs–Trade Partnership against Terrorism (C-TPAT) provides requirements for supply chain partners so they can be “trusted” to move cargo on land and across the ocean (Boske 2006).
5. Security and Accountability for Every (SAFE) Port Act, enacted in October 2006, sets the stage for the DHS to secure global trade movements through seaports by requiring 100% of all containers entering the United States to be scanned by nonintrusive technology, a significant issue presented next.

6. Secure Freight Initiative (SFI) is the pilot program intending to test SAFE's 100% requirement as scanning is ramped up across the globe (US GAO 2008).
7. The Megaports Initiative of the National Nuclear Security Administration, seeking to "equip 100 seaports with radiation detection systems by 2015, scanning approximately 50 percent of global maritime containerized cargo" (NNSA 2010). Also see "Glowing in the Dark," *The Economist*, December 14, 2013, pp. 67–68, for a discussion of global trafficking in radiological materials.

The SAFE Port Act confirmed previous initiatives, continued grant programs, but created more challenges for the supply chain than Congress anticipated. SAFE required 100% inspection of incoming containers, at the foreign port if possible, using the ISS with NII scanning technology. The statute obligated the DHS and ports to have 100% scanning in place by 2012. This apparent desirable security action sparked substantial resistance by global governments and the shipping industry as well as the DHS itself.

### 12.5.2 Great Scanning Debate

By necessity, the development of nonintrusive scanning technology was essential to serve dual objectives of security inspection and cargo productivity. If effective technology was available, then the immediate presumption is that every container would take advantage of the valuable scanning capability to identify illicit humans and materials. Yet an unexpected debate developed in the US Congress over the DHS's inspection strategy. Here is a summary of two approaches in battle:

1. *High-risk scanning*: Using an intelligence information system, the DHS and its CBP unit identify trusted shippers and cargo in advance. They determine high-risk or "untrusted" containers to be inspected at foreign ports of embarkation, hopefully minimizing the need to scan at US ports of debarkation.
2. *100% scanning*: The alternative approach, clearly a more complete barrier, is to scan every container at a foreign port or at a US port, assuming a highly effective scanning technology. Security technology requires large capital investments and generates fear that 100% scanning could significantly delay supply chain movements.

Either of these strategies can be successful at minimizing the vulnerability of port operations if correct estimates of cargo risk are available before inspection decisions. While Congress initially declared a winner in the battle by passing the 100% scanning statute, the legislation brought a chorus of resistors responding to the scanning requirement. Several strong opinions were put forth in 2010 as the 2012 deadline for 100% was nearing so Congress considered revisions to the original SAFE Port Act.

The European Union, through its European Commission, provided these arguments:

Strengthening the security of the supply chain via effective screening measures is a major European Union priority. Yet, implementing 100% scanning would require sizable investments, increase transport costs significantly and entail massive welfare losses. More importantly, such burdens to port authorities, companies and ultimately customers worldwide would be for no proven security benefit. (European Commission 2010)

Advocates for the supply chain industry called for the repeal of the 100% requirement:

Earl Agron of American Presidents Line (APL) said the law “should be reevaluated in terms of risk based measures targeting high-risk shipments...98% of containers entering US ports are scanned for radiation. Agron objects to the requirement that scanning be combined with X-ray imaging and detailed assessment of a container’s contents.” (Bowman 2010)

The layering (or integration) of risk-based and flexible methods like CSI, C-TPAT and SFI is the most effective way to address the very real and ever-changing risks within the global supply chain. (Berman 2010)

The World Shipping Council, a trade association for the liner shipping industry, took a stand by resisting security strategies that delay cargo:

The Industry is trying to construct meaningful security regimes that...do not unduly delay or restrict commerce or impose costs that produce little added security...however it supports well designed measures providing real security value. (World Shipping Council 2012)

This debate surfaced in 2005 before the original SAFE Port Act was passed. An article in the *Wall Street Journal* (WSJ) entitled “Keeping Cargo Safe from Terror: Hong Kong Port Project Scans All Containers; U. S. Doesn’t See the Need” provided a visual distinction between the two approaches (Price 2007, 572–573). The WSJ’s display suggested the three nonintrusive and separate scans using SAIC technology presented previously: X-ray, radiation, and OCR. All three scans were in one place, near pier side, inferring that all cargo could be passed through the scans directly after offloading, on the path taking them from the port. SAIC confirmed the Hong Kong demonstration in the 2009 manuscript with this statement (Orphan et al. 2009, 9):

‘ICIS can scan all inbound export containers...without impeding traffic...with information to help Customs identify high-risk containers for further inspection’. SAIC’s prototype ICIS system can scan export containers entering the terminal by truck or barge. With its high capacity, the system will handle the terminal’s full volume of up to 14,000 Twenty-Foot Equivalent Units per day

Interestingly, this author visited Hong Kong International Terminals (HKIT) in May 2008 and May 2013, finding scanning equipment available and HKIT indicating scanning is used when demanded by the US Customs. Yet the equipment was not placed in the direct path of container flow because not all containers required inspection by the United States or other nations.

### 12.5.3 Debate Continues

The 2012 deadline for 100% scanning came without implementation, sparking actions and proposals by the DHS itself, Congress, and two security critics.

First, the DHS took administrative action to avoid the 100% obligation:

...screening 100% of incoming containers would be nearly impossible to implement now...it's not necessarily a good use of resources to spend time and effort on ships that pose no risk. (Bliss 2012)

Under existing legislation, the DHS Secretary was able to grant a 2-year waiver from the requirement saying “the mandate is not practicable or affordable now.”

100% never meant a physical exam of each container, it referred to a risk-based screening of all cargo but only physical scanning when the CBP judge the risk ranking gives reason to scan 100%. (Straw 2011)

Congressional deliberations sought to support the DHS and its administrative position. In April 2011, S. 832 was introduced, called the *SAFE Port Reauthorization Act*, to update port security programs and, importantly, to adapt SAFE to allow less than 100% scanning. One provision states:

‘100% of containers originating outside the US undergo a screening to identify high-risk containers (via an intelligence data base and not a physical exam)...’. 100% of container identified as high risk are scanned or searched before entering the United States (assuming high risk determination ensures dangerous cargo is detected).

This remarkable change to the 2006 legislation languished in committee and has not received a vote by the Senate let alone the House. Such hesitance may be related to the general Congressional quagmire or may be caused by the inability to decide if the high-risk DHS strategy is an acceptable alternative to full scanning of containers.

The Congress also responded to the original SAFE Port Act by introducing S. 3639 in July 2010, *MTSA of 2010*, calling for containers to be scanned by “either nonintrusive imaging equipment or radiation detectors, leaving it to the ports to opt for one technology or the other.” The bill would also “extend the 100% requirement from 2012 to 2015 and allow DHS to further extend the deadline if 100% scanning is

deemed to be not feasible" (Edmonson 2010). This bill too died in the past congress, possibly signaling that the current DHS SAFE interpretation, waiver, and high-risk inspection methodology are acceptable to Congress. An apparent legislative consensus on 100% scanning may not stand as more knowledge is gained about terror risk and inspection strategies.

Two seaport security critics proposed alternative strategies. Stephen Flynn, defending the intent of SAFE, holds a slightly different strategy, beginning with the belief that "100% inspection is the only scheme to protect the shipping system." Flynn and two colleagues presented a study, released in 2011, using a simulation to test a compromise strategy to enhance screening. The following is a brief description of their scanning proposal (Flynn et al. 2011):

Under this scheme every container arriving at a terminal immediately undergoes a higher capacity drive through primary inspection for nuclear material. Those containers that trigger an alarm at primary inspection are tagged for a more careful secondary inspection where their dwell time is available to complete the inspection.

Flynn et al. call this an industry-centric scheme because they intend:

Terminal operators take responsibility for purchasing, deploying and operations inspection equipment, with the US government establishing standards for inspection processes and equipment and ensuring effective operation.

Jim Giermanski (2013), a transportation security consultant, offers another proposal. He begins by restating language from SAFE legislation in 2006/2007:

...a container loaded on a vessel in a foreign port shall not enter the United States unless scanned by nonintrusive imaging and radiation detection equipment at the foreign port...all containers entering the United States...by vessel shall be scanned for radiation...deploying next generation radiation detection technology.

Giermanski then specifies advanced radiation detectors and in-container sensors. His challenge is to ensure radiation is detected by evolving technology, given these nuclear materials are readily available, easy to assemble, and shielded in transit:

US ports utilize PVT (polyvinyl toluene) portal machines very good at detecting radiation from materials such as ceramic tile but not highly enriched or shielded uranium

...Congress is expecting new technology to be commercialized to detect dangerous radiation...these new machines, called Advanced Spectroscopic Portals (ASP) have not yet been developed

In fact, using in-container sensors and communication platforms allows us to detect shielded enriched uranium today

...the fix is simple. With respect to the use of "at" seaports, Congress merely has to amend the Acts to allow for the alternative use of in-container systems of detection and reporting.

The administration has made a choice for now while the legislature continues to waffle on the inspection strategy—albeit 100% scan remains the law even though a provision allows for the waiver. No one is legally challenging the DHS on the 100% mandate, for port operators and logistics carriers will certainly not fight the existing situation. The prototal screening interests have not carried the day in legislation or chosen litigation, instead keeping active through news and publications. The debate over security effectiveness versus cargo productivity also needs to be clarified, more likely as seaport security gains more experience.

If financial responsibility for technology development and operation is shifted to supply chain actors, the more interesting question is whether security strategies and results will be different than under national influence. The federal government should want to reduce the risk of a terror event because the occurrence of a terror-caused disaster has very negative political ramifications. Yet if security decisions and investments become the burden of the global supply chain, we all pay for terror prevention in product cost rather than in federal taxation.

## 12.6 RESEARCH NEEDS

As inferred by the previous discussion, there is much to learn about seaport security if secrecy does not inhibit researchers from obtaining complete knowledge. Supply chain operators and security professionals deserve adequate information to support commitments to security resources and financially justify investments. So the most critical needs are to answer questions about the “ideal share of containers to scan” based on understanding the methodology used to place containers on the “high-risk ranking.”

### 12.6.1 Ideal Scanning Share

In 2005, the *WSJ* article introduced earlier suggested that 5.4% of containers were inspected under the US regime demonstrated earlier. More recently, Stephen Flynn quoted from the CBP webpage that stated, “5–6% of containers may pose a risk that warrants closer review at international ports” (Flynn et al. 2011). No attempt has been made to gather historical data on the share of containers currently being scanned by an integrated system, but likely it is small and certainly less than 10% at any time. How does this percentage matter to the continuing debate on scanning?

The ideal percentage will vary with the magnitude of terror efforts, but applying the correct share at the right time is the essence of the methodology. Logically, an optimal inspection share will capture all dangerous shipments/cargoes present at that time, reducing actual risk of terror success to zero if the methodology is valid. The scanning rate should increase when the threat is actually higher. The rate is raised too high when Type I errors create excessive cargo intervention, although these errors provide a safety margin needed with uncertainty in the method. If the scanning rate is too low, Type II errors increase as well as the probability of a successful terror event with consequences. The public ought to know more about this tolerance for

risk; how far down the risk-ranking containers inspection/scanning is necessary. A deliberate choice to err on the side of more scans may well be broadly acceptable to those threatened by terror, if not the ports.

The responsibility for determining container risk remains with the DHS and the National Targeting Center, but should their method be openly tested and improved? Those security leaders who believe the only strategy to avoid terror risk is 100% scanning cannot be confident of any share chosen, and the logical arguments just made are not convincing. Still, it remains possible that seaport cargo security can be achieved by limited inspection if the risk methodology is valid. No one would disagree that 100% scanning is an overreach, but the strategy hopes to assure the United States is not a victim of its own weak methodology.

### **12.6.2 High-Risk Methodology**

The intelligence methodology for establishing “high-risk” cargo relies on gathering information in advance on shipments and using a valid “risk screening process” to rank the container traffic. In testimony before Congress, the World Shipping Council presented the case for continued vigilance (World Shipping Council 2012):

The 24 Hour Rule requires electronic submission of ten cargo data elements 24 hours before loading plus vessel stowage plans as well as container status messages 24 hour before arriving in the US.

This “10 plus 2” initiative substantially improves cargo risk assessment and screening preformed by the National Targeting Center...advance cargo risk assessment is the most prudent and effective approach the US government can take...the government needs sufficient data to be confident of the system’s value and effectiveness.

Vigilance against security risks requires prudent security measures and the continuing enhancement of such measures as the risks change.

By 2014, it appears these challenges are still not answered, requiring trust in the National Targeting Center. Transparency may address the trust question but needed insight cannot be provided if secrecy rules. If the DHS is convinced more openness provides a terrorist advantage, then faith must prevail and true risk remains unknown to those impacted by terror.

### **12.6.3 Research Summary**

Researchers should be quite anxious to pursue seaport security since there is much to learn about barriers, technology capability, scanning strategies, and port vulnerability. National Laboratories’ technology development and analyses by the National Targeting Center are essential sources. Nuclear threats and policies are captured by a series of Nuclear Security Summits, bringing nations together to discuss nuclear material wandering across the globe (NSS 2014). Besides supply chain actors, critics, and national and international sources mentioned earlier, several comprehensive treatments of maritime and supply chain security can aid

research and strategic choices (Fong 2008; Christopher 2009; Caldwell 2010; Obama 2012).

This seaport security discussion is summarized by an agenda of research opportunities. Knowledge can be gathered and shared with governments, ports, supply chain operators, and public interests that seek to prevent terror impacts:

*1. Method for high-risk container determination*

Insight is needed into the method DHS uses to rank container movements on the high-risk list that seems essential to defend container scans ordered at foreign or US ports. How far down the container risk list should scanning be required to minimize the probability of a successful terror event and essentially what share of cargo must be scanned at any time as terror expectations ebb and flow?

*2. Port layout, cargo paths, and scanning*

Modeling a seaport's layout of infrastructure, equipment, and cargo paths across the port's logistics segment is a visually powerful tool for security decisions. Is security scanning in the direct path of cargo or shifted to a diversion? Again, the achievement of twin goals of security effectiveness and cargo productivity should be evaluated.

*3. Resulting port vulnerability to terror*

While the federal government and seaports have conducted some analysis, there is a continuing need to measure security barriers, scanning volume and technology effectiveness to predict seaport vulnerability. Assurance is also sought that foreign ports and global logistics partners are trusted to add a layer of defense to the security barrier.

*4. Port operators' responsibility for security obligations*

The ideal port security strategy is based on a consensus among all port actors regarding security initiatives and each actor's role. Private operators must effectively manage security of their operations, particularly given the consequences to facilities and cargoes. Do supply chain operators resist security measures because of ineffective scanning, impacts on productivity, or the burdens of security costs?

*5. Financial sufficiency to ensure security*

Given an agreed security initiative, is sufficient funding available to achieve strategic security objectives? Typical in any effort to avoid disaster is the question of whether logical and rational prevention plans are avoided or inadequately financed. Financial sufficiency is less likely when the responsibility is unspecified between national governments, seaports, and logistics partners.

#### **12.6.4 Final Word**

This chapter generated insights about ports, modal operations, and security, recognizing the substantial economic role seaports play in the global supply chain. No one should accept serious harm and disruptions anywhere in the world from terror events, even if the probability is small or port actors have concern about technology and

cargo delays. Prevention of terror consequences always requires continuing imagination for improvement of defense barriers and enhancement of inspection methods. Too often, terrorists “out-imagine” us, as history demonstrates, showing more commitment to attack than we devote to prevention.

All those involved with trade through seaports should have knowledge of the threat and detail on system effectiveness as well as evidence supporting the resulting vulnerability of their facilities and assets. Supply chain partners may resist security because they believe it reduces competitiveness, yet disaster surely limits their advantage. The responsibility for global terror will always be borne by national governments at war with terrorists, although today security is an added responsibility of all involved in globalization.

## REFERENCES

- Berman, Jeff. 2010. “Many Challenges Remain When it comes to 100% Ocean Container Scanning,” *Supply Chain Management Review*, August 4, 2010.
- Bliss, Jeff. 2012. “US Backs Off All-Cargo Scanning Goal with Inspection at 4%,” *Bloomberg.com/news*, August 13, 2012.
- Boske, Leigh. 2006. “*Port and Supply Chain Security Initiatives in the US and Abroad*,” prepared for the Congressional Research Service by the Lyndon B. Johnson School of Public Affairs, Policy Research Project, Report No. 150.
- Bowman, Robert J. 2010. “Why 100% Container Scanning Won’t Work,” *Supply Chain Brain*, a Think Tank, August 10, 2010.
- Caldwell, Stephen. 2010. *Maritime Security: DHS Progress and Challenges in Key Areas of Port Security*. GAO-10-940T. Washington, DC: US Government Accountability Office.
- Christopher, Kenneth. 2009. *Port Security Management*, Boca Raton, FL: CRC Press.
- Edmonson, R. G. 2010. “Senate Bill Would Modify Container Scanning,” *Journal of Commerce*, July 27, 2010 and “Congressional Trust,” *Journal of Commerce*, July 5, 2010.
- European Commission. 2010. “Secure Trade and 100% Scanning of Containers,” foreword by Algirdas Semeta, European Commission Staff Working Paper. Brussels, Belgium, February 2010.
- Fernandez, Miguel Omar Tovar. 2009. “The 100% Container Scanning Legislation: An Analysis of Waiting Lines and Economic Costs,” Thesis on Maritime Economics and Logistics. Rotterdam: ECORYS Nederland BV.
- Flynn, Stephen. 2004. *America the Vulnerable: How our Government is Failing to Protect Us from Terrorism*, New York: Harper-Collins.
- Flynn, Stephen. 2005. “US Port Security and the Global War on Terror,” *The American Interest*, Autumn.
- Flynn, Stephen. 2007. *The Edge of Disaster: Rebuilding a Resilient Nation*, New York: Random House.
- Flynn, Stephen, Bakshi, Nitin, Gans, Noah. 2011. “Estimating the Operational Impact of Container Inspection at International Ports,” Working Paper 2009-05-01, Risk Management and Decision Processing Center, Wharton School, University of Pennsylvania, published in *Management Science*, 57 (1), pp. 1–20.

- Fong, Robert. 2008. "Review of Maritime Security: An Introduction," a text by McNicholas, Michael, Elsevier, 2008, *Journal of Homeland Security and Emergency Management*, 5 (1), 1–5, Article 44.
- Giermanski, Jim. 2013. Powers International, recovered from his blog at SecurityInfoWatch.com, accessed on March 7, 2015.
- Haimes, Yacov. 2002. "Risk of Terrorism to Cyber-Physical and Organizational-Societal Infrastructure," *Public Works Management and Policy*, 6 (4), pp. 231–240.
- Haveman, Jon, Jennings, Ethan, Shatz, Howard, and Wright, Greg. 2007. "The Container Security Initiative (CSI) and Ocean Container Threats," *Journal of Homeland Security and Emergency Management*, 4, (1), 1–19, Article 1.
- Levinson, Marc. 2006. *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger*, Princeton, NJ: Princeton University Press.
- Meissner, Caryn. 2010. "Imaging Cargo's Inner Secrets," *Science and Technology Review*, Lawrence Livermore National Laboratory, January/February, pp. 17–19.
- National Nuclear Security Administration (NNSA). 2010. *The Megaports Initiative*, nmsa.energy.gov/Megaports initiative, September 2010.
- NSS. 2014. The Fifth Nuclear Security Summit (NSS) was held March 24–25, 2014 at The Hague, in Hague Center for Strategic Studies (HCSS). HCSS has published *Nuclear Timeline*, Tracing the "long legacy of nuclear security."
- Obama, Barack. 2012. "National Strategy for Global Supply Chain Security," The White House, January 23, 2012.
- Orphan, Victor, Muenchau, Ernie, Gormley Jerry, and Richardson, Rex. 2009. "Advanced Cargo Container Scanning Technology Development," Science Applications International Corporation, San Diego, CA, presented at Transportation Research Board (TRB) Annual Conference, Washington, DC.
- Price, Willard. 2004. "Reducing the Risk of Terror Events at Seaports," *Review of Policy Research*, 21 (3), pp. 329–349.
- Price, Willard. 2007. "Seaport Security from Terror: Risk and Responsibility," in Jeremy Plant, Editor, *Handbook of Transportation Policy and Administration*, Boca Raton, FL: Taylor and Francis Group.
- Radiation Portal Monitor (RPM). 2013. <http://en.Wikipedia.org/wiki/RadiationPortalMonitor>, accessed on March 7, 2015.
- Science Applications International Corporation (SAIC). 2013. [www.saic.com/media/27184/IS3-Brochure.pdf](http://www.saic.com/media/27184/IS3-Brochure.pdf); [www.comfleet.com/pages/CargoInspection/SAIC\\_ICIS\\_Page.html](http://www.comfleet.com/pages/CargoInspection/SAIC_ICIS_Page.html), accessed on January 20, 2013.
- Straw, Joseph. 2011. "Outlook for Container Scanning," *Security Management*. [www.securitymanagement.com](http://www.securitymanagement.com), accessed on March 7, 2015.
- US Government Accountability Office. 2008. "Supply Chain Security." GAO-08-187. Washington, DC: US Government Accountability Office.
- World Shipping Council. 2012. Testimony before the House Committee on Transportation and Infrastructure subcommittee on Coast Guard and Maritime Transportation on the "Tenth Anniversary of the Maritime Transportation Security Act: Are We Safer," September 11, 2012, Washington, DC and Brussels.
- Zakaria, Fareed. 2013. "Resiliency and Complacency," *Time's Special Tablet Edition on Boston's Bombing*, April 18, 2013.



---

# 13

---

## PATHOLOGIES OF PRIVATIZATION IN THE TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL PROGRAM

BENJAMIN INMAN AND JOHN C. MORRIS

*School of Public Service, Old Dominion University, Norfolk, VA, USA*

### 13.1 INTRODUCTION

This research examines the implementation of the Transportation Worker Identification Credential (TWIC) program. A program instituted in the post-9/11 era by the US Department of Homeland Security (USDHS), the TWIC is designed to keep unauthorized personnel out of sensitive maritime port facilities to protect these facilities from terrorism. Whereas the Transportation Security Administration (TSA) brought airline security back under government control, the TWIC program, also under the auspices of the USDHS, contains a significant portion of private sector involvement, particularly in the screening of applicants and production of the appropriate credential. We examined the TWIC program to determine whether the privatization apparent in the program has resulted in the creation of market failures, thus fitting Morris' (2007) definition of "pathologies of privatization."

The administration of a federal program can be accomplished by several methods: government administration, a privatized (contracted) service, or a hybrid contractual arrangement such as public–nonprofit partnership. The TWIC program presents possibilities that may occur when a critical portion of a national security program is

outsourced to a private contractor. In analyzing the data, we identified several areas that support theories on privatization and identified a potential area for theory development that is not present in public administration literature.

While Morris (2007) found evidence of these pathologies in the privatization of prisons, little other work has been done to determine whether similar pathologies can be found in other programs. This chapter extends the earlier work in a quest to identify the occurrences of these or other pathologies of privatization and their impact in the case of the TWIC program. The study was conducted in the Port of Hampton Roads, one of the largest natural harbors in the world. Hampton Roads is home to the US Navy Atlantic Fleet, cargo container terminals, and ship building and repair facilities. As the TWIC program only covered Maritime Transportation Security Act (MTSA) facilities, we examined the Port of Virginia, which includes the Norfolk International Terminals (NIT), Portsmouth Marine Terminal (PMT), and Newport News Marine Terminal.

### **13.1.1 The TWIC Program**

The primary goal of the TWIC program was to determine security threats to the maritime transportation systems of the United States and prevent unauthorized access to secured and restricted facilities. Providing for national security is an inherent function of government that is generally not relinquished to the private sector.<sup>1</sup> The initial intent of the TWIC program was to cover both maritime and aviation under one system; instead, aviation terminals successfully deployed credentials to hundreds of thousands of workers in a short amount of time (Monroe 2007). Meanwhile, the maritime transportation industry had gone almost a decade without a successful and fully secure system in maritime transportation.

The TWIC program was established in December 2001 to prevent unauthorized access, by terrorists or other unauthorized persons, to secure areas of the transportation network by the creation and implementation of a federal common identification credential. The enactment of the MTSA of 2002 solidified the requirement by tasking the USDHS with the issuance of a biometric encoded credential to workers in the maritime transportation industry and would be later known as the TWIC. The TWIC is a biometric, smart card-based common identification credential for personnel requiring unescorted access to all MTSA regulated facilities. The intent of the credential is to support multiple layers of cardholder authentication, which included a photograph, a unique pin number, and biometric information.

### **13.1.2 Historical Background: Implementation**

The USDHS' responsibilities for implementing the program were split between two agencies (Haveman et al. 2005), the TSA and the US Coast Guard (USCG). The TSA is responsible for the TWIC enrollment, security threat assessment and adjudication,

<sup>1</sup>We note the trend toward the use of private contractors to provide ancillary security support in both Iraq and Afghanistan. However, it is important to note that combat operations are performed by uniformed soldiers acting as part of national forces and thus exercise the coercive power of the state.

card production and issuance, and the appeals and waiver process. The USCG took on the enforcement role of the program and is responsible for enforcing the use of TWIC at all MTSA regulated facilities (Bilisoly 2007). The planning phase, or phase I, spanned spring 2002 to spring 2003. Phase II of the TWIC program, the technology evaluation period, performed by Maximus Inc., ran from the fall 2003 to fall 2004. Maximus Inc. was later contracted by Lockheed Martin to serve as the web master for the TWIC program.

In August 2004, the TWIC pilot program was launched to test the program at 28 transportation facilities across the United States (GAO 2008). The USDHS outsourced the test and evaluation of the TWIC pilot program to BearingPoint Inc., the world's largest system integration company, for \$12 million and, after several delays and extensions, nearly doubled the contract value to \$24.5 million. BearingPoint, also significantly involved in the Department of Defense Common Access Card program, provided the TSA with direction on the initial enrollment process for the TWIC program.

On January 25, 2007, the TSA and the USCG released the first of two TWIC rules. Rule one established the regulatory requirements for TWIC enrollment and card issuance regulations to the maritime community. The rule established that all members of the maritime transportation community, estimated at 750,000 workers, that require unescorted access to a MTSA regulated facility and or vessel must have been vetted for security threats and issued a TWIC. In addition, the rule mandated a change in the security operating procedures of the MTSA regulated facilities and vessels to ensure that all non-TWIC holders were denied unescorted access to secure areas of the facilities.

On January 29, 2007, the USDHS awarded the initial full deployment contract for the TWIC program to Lockheed Martin Corporation—Transportation and Security Solutions. The initial indefinite delivery/indefinite quantity contract for the deployment of the TWIC program to the various ports was worth \$70 million (Hawley 2007). Under the terms of the contract, Lockheed Martin, through various subcontractors, provided enrollment centers in close proximity to the maritime port facilities. Each applicant reported to one of the TWIC offices to provide their biometric and identifying information. For the Hampton Roads area, Senture Security Solutions was subcontracted to provide the staffing and enrollment centers.

The full implementation date of the TWIC program was originally scheduled to occur on September 25, 2008. The TSA opened the enrollment centers for the TWIC some 6 months behind schedule. The delay prompted the TSA and USCG to allow additional time to process the TWICs. Due to problems and delays with the program, the final compliance date, or national deadline, for the TWIC was extended until April 15, 2009. The USCG phased in the compliance by way of rolling dates for the 45 Captain of the Port (COTP<sup>2</sup>) zones. On April 15, 2009, all personnel that required unescorted access to secure areas of vessels and facilities that are regulated by the MTSA of 2002 were required to have the TWIC (33. CFR. Part 105).

<sup>2</sup>The Captain of the Port is a senior Coast Guard officer who is responsible for all operational aspects of a commercial port, from port operation to safety and security. COPT offices are located in all major port cities in the United States.

### 13.2 PATHOLOGIES OF PRIVATIZATION

Pathologies of privatization can occur when an attempt to cure one failure results in another failure. Government contracting is illustrative of this problem. Detractors of government often contend that when government provides, produces, or delivers a good or service, government often holds a monopoly on that good or service. If the good or service is bid to the private sector, the forces of competition will come into play; as a result, price will go down and quality will rise. However, prices go down the most when the term of the contract is longer, particularly when the good or service requires capital-intensive infrastructure (see Heilman and Johnson 1992; Morris 2007). A long-term contract gives the winning business a great deal of certainty and makes capital-intensive projects, such as private prisons, financially feasible. However, contracting effectively replaces one monopoly (government) with another (private sector) monopoly. While there may be competition for the initial contract, the ultimate result is still a long-term private sector monopoly (and one protected under contract by government). This also precludes government from realizing any benefits from changes in technology, market structure (e.g., number of competitors, etc.), or other factors for the life of the contract—it may be possible to be even more efficient, but there is no incentive for the monopoly (contract) holder to innovate. Also, the contractor has an incentive to improve service delivery beyond the requirements of the contract in order to get a renewal.

Likewise, proponents of privatization are often quick to note the negative effect of civil service protections on government efficiency and effectiveness. Contracting the good or service, they argue, will rid the good or service of these expensive protections, thus lowering costs. However, a staple of government contracting are a long series of crosscutting laws and regulations to which contractors must agree to adhere in order to be eligible to bid on contracts. Usually, pensions and retiree healthcare costs are significantly lower than government's. Whether wage laws, family leave, or fair hiring practice guarantees, these crosscutters place significant costs on private companies wishing to do business with government. Moreover, these laws are not capricious or trivial; they exist to correct historical (and prevent future) abuses on the part of businesses. In short, we may privatize to avoid civil service costs, only to saddle our private sector partners with different kinds of personnel costs.

Finally, much of what government produces has no economic value outside of the narrow context of the good or service itself. This situation makes it difficult, if not impossible, to place a monetary value on that good or service. Whereas businesses can calculate efficiency and profit by comparing inputs to outputs (or costs to revenues), no such measurement exists for most of what government provides citizens. This is especially true when the service is an administrative function. Administering a program may be something that can be done by either the public or the private sector, but how does one measure the efficiency (Morris 2007)? Indeed, what is the output? Contracts must be very detailed with respect to performance. Usually, the required performance is that of the state-run programs. Likewise, we can privatize the caseworker function for welfare applicants (see Breaux et al. 2002), but how does one measure the efficiency (or the quality) of such services? Moreover, Morris (1997)

shows that turning over the administration of a public program can significantly change the distribution patterns of the goods or services delivered, yet any distribution pattern clearly has a value to both recipients and nonrecipients. In effect, we solve the problem of a difficulty in valuing outputs by contracting the task to a private company, but private companies in this instance are no more able to value their output than is government. The result is typically a contract based on the number of clients served (or, worse, a fixed-price contract that pays the same regardless of the number of clients served). This often creates a market failure—the private company knows how much it actually costs to provide the administrative services, but this information is almost never shared with the government. In this case, we simply trade a government failure for a market failure in a false quest for efficiency. Equally important is the difficulty privatizing the programs that delegate rights inherently reserved for the state (government).

### 13.3 EVALUATION

#### 13.3.1 Problems in the TWIC Program

The TWIC program saw various problems from its inception. The initial intent of the TWIC program was to cover both maritime and aviation under one system; instead, aviation terminals successfully deployed a credential to hundreds of thousands of workers in a short amount of time (Monroe 2007). Meanwhile, the maritime transportation industry has gone seven plus years without a successful program. There were concerns brought by stakeholders, specifically AFL-CIO members, that the TWIC system would unduly disqualify workers with criminal histories and determine them to be security risks (Willis 2007). This was later confirmed by the experiences of hundreds of workers that were initially disqualified without a disqualifying offense (Moskowitz 2008). There was also a consensus among the nation's port security directors that the TWIC process had significant problems with the biometric fingerprint readers; there were a lack of communication and inconsistent information about the requirements for enrollment and little to no outreach to the various stakeholders (Bowman 2008).

#### 13.3.2 Problems Inherent in Decentralization

The United States, as well as many other democratic governments, has a highly decentralized system of government (Weimer and Vining 1992). Highly decentralized government, however, often experiences problems with policy implementation due to the deference of authority to lower levels of government or the various other stakeholders in the program (see Pressman and Wildavsky 1984). The TWIC program is the largest single national security initiative following the largest consolidation and reorganization of federal national security agencies (GAO 2003), with the exception of the formation of the Department of Defense, in the US history. The consolidation of the 22 federal agencies that now comprise the USDHS stretched the capabilities of

the new agency that necessitated the department to turn to the market to provide a variety of functions in the TWIC program.

In the case of the TWIC program, decentralization was found in both the government and privately run operations. The TSA examined two program alternatives. The first, centralized, alternative was a federal program designed and implemented by the national government. The second, decentralized, approach was a program designed and managed by each individual port (GAO 2005, 6–7). In the end, the TSA would provide the TWIC, through a contractor, and the local entities would supply the equipment to read the TWIC.

The implementation of the TWIC program was split between two agencies that fall under the USDHS. The TSA, formerly a component of the Department of Transportation, was tasked with the development, testing, and issuance of the TWIC, as well as the development and maintenance of the “Hot List” (GAO 2005). The “Hot List” was a list of individuals that were excluded from access into maritime transportation facilities. The USCG would take on the enforcement role of the program since the agency was responsible for the overall security of the US maritime transportation system (GAO 2003). The increased layers of decentralization created a perception of miscommunication and misinformation between the various levels of government, the contractor, and subcontractors. Essentially, an insulation effect occurs when a contractor utilizes a subcontractor to provide the good or service on behalf of the contractor. The use of a subcontractor has the potential to break down the communication streams to where it is very difficult to work with program officials. The TWIC program increased the problems of decentralization, a government failure, through the privatization of the TWIC program, which created additional layers that spanned the USDHS, TSA, Lockheed Martin, and the various subcontractors. The market failure in turn created significant principal–agent accountability problems that required increased monitoring mechanisms. The GAO identified this problem in a series of reports spanning the TWIC program from 2005 to 2008. In 2005, GAO concluded that poor planning for the initial testing contract created extensive delays and contract changes (GAO 2005). These delays and contract changes doubled the cost of the testing from the initial contract of \$12 million to the final contract cost of over \$27 million (GAO 2005). Likewise, the reports (GAO 2005, 2006) also noted that future contracts with the program would need to be extensively monitored by the TSA and USDHS. In addition to the need for increased accountability mechanisms, the principal–agent problem also led to increasing information asymmetry.

### 13.3.3 Problems Inherent in Bureaucratic Supply

One of the largest government failures identified in the TWIC program is that of bureaucratic supply or, more specifically, valuing the output of the program. Securing the nation’s transportation system is extremely complicated and must strike a balance between security and commerce flow (GAO 2008). The USDHS must consider the burden of the TWIC program on the daily flow of commerce (GAO 2006).

By April 14, 2009, all of the COTP zones were in full TWIC compliance. The problems in the system left thousands of port workers without TWICs and later

without jobs. Approximately 10,000 workers had lost their jobs, while the April 14th compliance deadline passed and the TSA had not made the final decision on the their TWIC applications (Ensellem et al. 2009, 3). The program was unable to determine if the applicants, or port workers, were actual security threats, which would indicate that the government failed to provide for the national security of its citizens. In many cases, these port workers had been employed in the same capacity, at the same port, after prior convictions without incident. A large number of the delays were based on ineffective screening methods employed by the TSA. The initial determinations of individual TWIC eligibility averaged approximately 4 months, and individuals that challenged the initial denial waited an average of 7 months to receive their TWIC (Ensellem et al. 2009). In the case of security threat determinations, the TSA did not provide adequate resources to efficiently and effectively screen the backgrounds of port workers applying for the TWIC. The TWIC program exempted certain types of marine terminal facilities. In Hampton Roads, Newport News Shipyard and Northrop Grumman were not required to adhere to the TWIC program. Both of the marine facilities handle nuclear materials used to fuel the US Navy vessels that they build and/or service. Excluding critical infrastructure facilities from the program leads to questions to the veracity of the TWIC program.

Hampton Roads saw little if any changes in the maritime workforce post-TWIC. Little to no change in the workforce of one of the largest maritime seaports in the country would indicate that there are either few security threats to the facilities or the TWIC program was ineffective at determining who was a security threat. For example, would an individual that was convicted of murder 20 years prior, served their sentence, and has returned to work at a maritime facility for the next 15 years without an issue be considered a security threat? In the case of TWIC, the individual would be considered a security threat even though there is no connection to terrorism. A National Employment Law Project (2009) confirmed that almost 100% of those applications that were disqualified from obtaining a TWIC were later approved during the appeal process. These applications had disqualifying felony convictions; however, the individual proved to the TSA that they were not terrorist threats to the maritime industry.

There are several possibilities that may explain the high percentage of overturned disqualifications. First, there were relatively few security threats present in the existing maritime transportation workforce. In terms of those individuals that were initially disqualified, the vast majority seemed to have been successful in the appeal process. So on the one hand, you disqualify an individual based on the criteria that were originally put in place to minimize security threats, and on the other hand, the appeal process allowed those that were disqualified an avenue of redress. Those that were disqualified and were not successful with their appeals may have been excluded from the TWIC because of unrelated crimes to terrorist activities. The legislation guiding TWIC was written to deny access to secure areas of the nation's maritime critical infrastructure. The regulations as implemented from the regulations excluded those that had violent convictions in their past. In many cases, the person that was excluded had received an exemption. To begin with, the individual could not have been considered a terrorist because they had been previously convicted of a violent

crime. The criteria used for adjudicating the disqualifying offenses were too moderate. Possibility one, very positive for national security, would indicate that the program was unnecessary. The other possibility lends concern that the criteria used for disqualifications or the appeals process may have been too lenient to be beneficial. These problems all stem from the inability to effectively gauge the output of the service of the program.

Deficiencies in the market that prevent efficiency and effectiveness often result in failure to provide a good or service (Morris 2007). Unlike most services, a failure in the area of national security can have severe implications as witnessed during the implementation of the TWIC program. Typically, the unsuccessful provision of a good or service would be deemed a government failure; however, a large portion of the TWIC program was privatized, which traded the government failure of bureaucratic supply for the binary market failures of information asymmetry and a natural monopoly. The motives of the market often outweigh the program's intent (output), and therefore, the market is driven to provide less information to gain further compensation. Since a natural monopoly exists, consumers are unable to look to alternate sources of service provision to overcome the deficiency. The TWIC program was designed to prevent security threats, or those individuals that did not have a valid TWIC, from entering the secure and restricted MTSA regulated facilities. Likewise, the program's intent was to ensure that qualified applicants for the TWIC were granted access to their job sites.

Making the determination on what offenses qualify as threats to the security of the nation's maritime transportation infrastructure is no easy task. The valuation of the output has implications on both ends of the spectrum. Including more disqualifying offenses in the threat assessment means more individuals are excluded from the industry even if they do not represent security threats, while decreasing the severity of disqualifiers may threaten the maritime transportation infrastructure. The TWIC program has taken the uncertainties of this government failure and passed them to the primary contractor, which in turn is unable to gauge the output and therefore likely to assume any inefficiency that would have occurred through government provision. Likewise, problems with valuation of the output also allow for rent-seeking behaviors on the part of the contractor.

The primary contractor for the TWIC program, Lockheed Martin, was responsible for ensuring all details of the program were adequately communicated to the industry stakeholders. There was significant criticism that the contractor neither provided information on the appeals and waiver process of the program nor explained permanent disqualifying offenses to TWIC applicants. Failure to disclose permanent disqualifying offenses would allow the contractor to collect fees for applications without incurring the additional costs of producing, shipping, and issuing the credential since the individual would not be eligible for the TWIC at the onset of the application process. The fees required for the TWIC are paid prior to the commencement of any service provision; that is, the TWIC application process will not start until the applicant has paid the \$132.50 application fee. The fee for the TWIC is not contingent upon successful completion of the security threat assessment and card production, but rather, the fee is contingent upon application submission. Essentially,

the contractor could allow individuals who they know have disqualifying factors to apply for the TWIC. The service has been technically rendered to the end user and the fees collected; however, the service does not meet the intent of the program. Since the government has difficulty valuing the output of the program, it can very easily pass the problem to the market.

### **13.3.4 Information Asymmetry**

On October 21, 2008, the facility that housed the TWIC system suffered a catastrophic power outage that crippled the program's ability to activate TWIC cards (PAC 07-08). The system was not fully restored until November 10, 2008, and created significant TWIC activation delays as the COTP zones came closer to the compliance date. The problem was caused by the contractors' failure to implement redundant safeguards to preserve power during possible power outages. The outage damaged the only system that was capable of activating TWICs. In addition, the contractor also lost the TWIC enrollments of roughly 3000 port workers when the contractor accidentally used the training program for enrollments in lieu of the actual program. In a December 2008 letter to Michael Chertoff, secretary of the DHS, Representative Bennie Thompson (D-MS) indicated that there were several problems that the Homeland Security Oversight Committee was aware of including the loss of 3000 TWIC records (Thompson 2008). The contractor mistakenly utilized the wrong enrollment application for processing port workers' TWIC applications. The information gathered through the lengthy enrollment procedure was never processed and left the applicants with the impression that they would soon receive their TWIC. No information was relayed to the individuals or the principle regarding the incident, and workers were unable to determine the application status through the Help Desk. On the other hand, payment was rendered for the application process even though the process had not been started.

Under the TWIC contract, Lockheed Martin was required to develop and provide an effective communication plan to ensure that major stakeholders were apprised of key program details and provided a mechanism for input. Like many other aspects of the program, the communication from the contractor to the industry stakeholders was lacking (Himber 2007). There was an abundance of "misinformation and inaccurate rumors abound about the TWIC eligibility requirements" (Mokowitz 2008, 2). A large number of workers applied for the TWIC program that had criminal convictions; however, they were not disqualifying offenses. Those that had possible disqualifying offenses were unaware that they could apply for a waiver if the initial determination denied the issuance of the TWIC. As Moskowitz (2008) pointed out in her testimony to the US House of Representatives Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Terrorism, the problems associated with TWIC implementation meant that many experienced port workers were denied their right to work. Information asymmetry not only created principal-agent problems; in the case of the TWIC program, it also excluded long-time port workers from the maritime industry. Since the service was provided by one company, there was no choice for workers to seek alternate sources for applying for the TWIC program.

### 13.3.5 Natural Monopoly

The TSA also substituted a bureaucratic supply problem, a government monopoly, for a natural market monopoly in outsourcing large portions of the TWIC program. The operational component of the TWIC program was outsourced as a “competitively bid, indefinite delivery/indefinite quantity contract to Lockheed Martin Corporation” (Hawley 2007, 5). Although a competitive bid process is undertaken, the indefinite delivery/indefinite quantity contract provides the contractor certain level of security within the market. In short, competition is limited and realizations of the efficiencies of privatization are significantly reduced. Essentially, the long-term, single provider contract created a natural monopoly that discourages competition, increased efficiency, and technology advancement.

### 13.3.6 Buffering

In analyzing the data, we have also identified a possible new phenomenon that could lead to the expansion of the “pathologies” framework. There were several statements made by one of our interviewees that would indicate that there is a buffering effect that occurs in contractual arrangement when the primary contractor subcontracts a portion of the service production. During the TWIC implementation in Hampton Roads, Lockheed Martin utilized a subcontractor to process the enrollments and activations for the TWIC cards. In the arrangement, the subcontractor was able to create a distance between Lockheed Martin and the general public. Senture was effectively placed to be the buffer. Although Senture seemingly received a significant amount of blame for the issues in Hampton Roads, they had little if any control on the overall process and could not affect any positive changes without Lockheed Martin.

We define buffering as an organizational arrangement created through multiple layers of contracting, by design, which will shelter or protect the primary contracting organization from bothersome routine matters, criticism, or responsibility for failure. Bothersome routine matters in this sense are stakeholder input and requests for assistance due to poor performance. The concept is similar to that of the problem of multilayered, or complex, principal–agent relationships, as described by Breaux et al. (2002). Like complex principal–agent models, buffering creates additional layers in the system, further decentralizes implementation systems, and makes accountability more difficult. The market failure of “buffering” is an inherent result of trading the government failure of bureaucratic supply, specifically that of decentralization, for a market failure of information asymmetry. The failure is compounded by the multiple stakeholders and principal–agent relationships that are present. Essentially, to correct for government decentralization, the privatized service arrangement, which includes a contractor and subcontractors, creates a market failure of decentralization. Like the decentralization found in the TWIC program that would create multiple layers of stakeholders, the program traded the decentralization of government for that of multiple layers of contractors and subcontractors. The primary issue that arises with the market pathology of buffering is that the increased layers of decentralization remove the primary contractors that are responsible for implementation from public scrutiny. Buffering would also create the need for additional accountability mechanisms to prevent further inefficiencies and information asymmetry. A more in-depth longitudinal study of the program may shed light on this phenomenon.

### 13.4 CONCLUSION

The TWIC program exhibits several pathologies of privatization. The pathologies include both government and market failures individually, as well as the hybrid arrangement of failing to differentiate between a government and the market failure. Although each failure is represented individually, there are indicators that support the pathologies of substituting one failure, whether market or government, for another.

The issue of port security is not trivial. In an age of international terrorism, one in which deficiencies in America's transportation security have already been exploited, the need for effective port security is very real. The Americans expect their government to keep both the population and its infrastructure safe, and the TWIC program is but one of many efforts to carry out this mandate. A Bush-era initiative, the TWIC program, like many other public policies of the era, is a reflection of the broader ideological and policy preferences of the times. Elements of privatization are contained in many of the policies of the Bush administration and are indicative of a philosophy of governance that the private sector can do many things better, and more efficiently, than the public sector. The inherent strengths of the private sector can (and should) be harnessed to provide traditionally public goods and services.

Our analysis of the TWIC program, however, suggests that privatization did not result in any particular efficiencies or increases in quality. Rather, the decision to privatize the TWIC program simply resulted in exchanging one set of (potential) government failures for a set of very real market failures. Part of the problem can probably be reasonably traced to a lack of effective government oversight. Donald Kettl (1993) argues that for privatization to be effective, government must act as a "smart buyer"; that is, they must understand what they want; they must choose a private sector partner with the proven abilities to deliver the desired goods or services; and they must effectively monitor the performance of that partner to assure that the product meets expectations. Although the first two conditions may have been met in the case of the TWIC program, the third condition was clearly not. Moreover, by allowing the prime contractor to subcontract important elements of the program, the government abdicated a significant portion of its "smart buyer" role to the private sector and was at the mercy of the prime contractor's interest and ability to act in the government's self-interest, as well as its own.

The issues inherent in the TWIC program are more than pathologies of privatization. While the use of this framework aids our understanding of the events of the TWIC program, the effects of these failures have real consequences for both individual citizens and our national security. The events of September 11, 2001, have ignited a heated debate in the United States about the balance between national security and individual rights. While that debate is often characterized as a zero-sum game (increases in one necessarily lead to decreases in the other), implementation of the TWIC program suggests that the involvement of the private sector actually results in a decrease in both national security and individual rights. Individual citizens are clearly being deprived of their fundamental rights by a private entity that exercises the coercive power of government, and yet our ports are not demonstrably safer (or better protected from terrorism) as a result of these actions. Although one might

reasonably point out that a fully government-operated program would have been any more successful, government's willingness to abdicate its responsibilities to the private sector has created its own set of failures and has made the program significantly less accountable to citizens.

We also find support for Morris' (2007) concept of "pathologies" of privatization. The TWIC program not only exhibits evidence of several of the pathologies already identified, but the additional pathology of "buffering" is created by subcontracting functions of the program. In essence, it appears that the traditional government failure of decentralization can also become a market failure of decentralization. Just as importantly for public policy goals, a market failure of decentralization in a privatized arrangement makes government monitoring, and ultimately accountability, that much more difficult to achieve. It remains the focus on ongoing research to determine whether other pathologies might be identified. At the moment, however, it appears that privatization is not a cure for government ills (Savas 2000), but is more likely to trade one set of problems (failures) for another. In the case of the TWIC program, the requirements of the MTSA of 2002 have yet to be filled. In the end, the TWIC program has yet to be fully implemented in regard to the use of biometric security features of the credential, feature that was touted as necessary to secure the maritime transportation infrastructure.

## REFERENCES

- Bilisoly, Nash F. 2007. *An Overview of the Transportation Worker Identification Credential (TWIC) Program & Related Preemptive Issues*. Norfolk, VA: Vandeventer Black LLP.
- Bowman, Stephanie. 2008. Transportation Worker Identification Credential: Hearing before the Border, Maritime and Global Counterterrorism Subcommittee of the House Homeland Security Committee. <http://www.gpo.gov/fdsys/pkg/CHRG-110hrg48090/html/CHRG-110hrg48090.htm> (accessed March 7, 2015).
- Breaux, David A., Christopher M. Duncan, C. Denise Keller, and John C. Morris. 2002. Welfare Reform, Mississippi Style: Temporary Assistance for Needy Families and the Search for Accountability. *Public Administration Review* 62(1): 92–103.
- Ensellem, Maurice, Laura Moskowitz, Madeline Neighly, and Jesse Warner. 2009. A Scorecard on the Post 9/11 Port Worker Background Checks: Model Worker Protections Provide a Lifeline for People of Color, While Major TSA Delays Leave Thousands Jobless During the Recession. National Employment Law Project, July 2009. <http://www.nelp.org/page/-/SCLP/PortWorkerBackgroundChecks.pdf?nocdn=1> (accessed March 7, 2015).
- Haveman, David, Howard Shatz, and Ernesto Vilchis. 2005. U.S. Port Security Policy after 9/11: Overview and Evaluation. *Journal of Homeland Security and Emergency Management* 2(4): 1–24.
- Hawley, Kip. 2007. Transportation Identification Credential (TWIC): Testimony before the United States House of Representatives, Committee on Homeland Security. <http://chsdemocrats.house.gov/SiteDocuments/20071101095233-35457.pdf> (accessed March 7, 2015).
- Heilman, John G. and Gerald W. Johnson. 1992. *The Politics of and Economics of Privatization: The Case of Wastewater Treatment*. Tuscaloosa, AL: University of Alabama Press.

- Himber, Lisa B. 2007. Homeland Security Failures: TWIC Examined. U.S. House of Representatives Committee on Homeland Security. <http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg48976/html/CHRG-110hhrg48976.htm> (accessed March 7, 2015).
- Kettl, Donald F. (1993). *Sharing Power: Public Governance and Private Markets*. Washington, DC: Brookings.
- Monroe, Jeffrey W. 2007. One Year Later: A Progress Report on the Security and Accountability For Every (SAFE) Port Act. United States Senate, 110th Congress, First Session. Committee on Homeland Security and Governmental Affairs. <http://www.gpo.gov/fdsys/pkg/CHRG-110shrg38849/html/CHRG-110shrg38849.htm> (accessed March 7, 2015).
- Morris, John C. 1997. The Distributional Impacts of Privatization in National Water Quality Policy. *Journal of Politics* 59 (1): 56–72.
- Morris, John C. 2007. Government and Market Pathologies of Privatization: The Case of Prison Privatization. *Politics & Policy* 35(2): 318–341.
- Moskowitz, Laura. 2008. Transportation Worker Identification Credential: A Status Update. U.S. House of Representatives Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Counterterrorism, September 17, 2008. <http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg48090/html/CHRG-110hhrg48090.htm> (accessed March 7, 2015).
- Pressman, Jeffrey L. and Aaron Wildavsky. 1984. *Implementation*, 3rd edn. Berkeley, CA: University of California Press.
- Savas, Emanuel S. 2000. *Privatization and Public–Private Partnerships*. Chatham, NJ: Chatham House.
- Thompson, Bennie G. 2008. A letter to the Honorable Michael Chertoff, Secretary of U.S. Department of Homeland Security (December 4, 2008).
- Title 33 CFR. Navigation and Navigable Waters: Chapter I. (July 1, 1999) United States Coast Guard. 4910-15-U.
- TWIC Final Rule 2008. Transportation Worker Identification Credential Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License. United States Coast Guard, Transportation Security Administration. Federal Register, Vol. 73, No. 190. September 30, 2008. Docket Nos. TSA-2006-24191; USCG-2006-24196.
- U.S. Government Accountability Office (GAO). 2003. Homeland Security: Challenges Facing the Coast Guard as it Transitions to the New Department. GAO-03-467T. Washington, DC: U.S. GAO.
- U.S. GAO. 2005. Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program. GAO-05-106. Washington, DC: U.S. GAO.
- U.S. GAO. 2006. Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program. GAO-06-982Washington, DC: U.S. GAO.
- U.S. GAO. 2008. Transportation Security: Transportation Worker Identification Credential: A Status Update. GAO-08-1151T. Washington, DC: U.S. GAO.
- Weimer, David L. and Aidan R. Vining. (1992). *Policy Analysis: Concepts and Cases*, 2nd ed. Upper Saddle River, NJ: Prentice Hall.
- Willis, Larry I. 2007. Transportation Worker Identification Cards: House of Representatives, 110th Congress, First Session. Subcommittee on Coast Guard and Maritime Transportation of the Committee on Transportation and Infrastructure. July 12, 2007. <http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg36689/html/CHRG-110hhrg36689.htm> (accessed March 7, 2015).



---

# 14

---

## TRAVELER'S SECURITY PERCEPTIONS AND PORT CHOICES

AMALIA POLYDOROPOULOU<sup>1</sup> AND ATHENA TSIRIMPA<sup>2</sup>

<sup>1</sup>*Department of Shipping Trade and Transport, University of the Aegean, Chios, Greece*

<sup>2</sup>*Transportation and Decision Making Laboratory, University of the Aegean, Chios, Greece*

### 14.1 INTRODUCTION

Transportation systems, due to the large passenger and goods volumes they convey, their relatively easy accessibility, as well as their diversity in ownership and management, have become the primary targets of terrorist attacks (Hardin 2004; Ito and Lee 2005; Jenkins and Butterworth 2007). The terrorist attacks at the New York twin towers (2001) and the ones in Madrid (2004), London (2005), and the Moscow Metro (2010) showcase the difficulty of protecting people against such actions, while the injuries and damages caused by such attacks have a great impact both on the public's psychology and on government policy.

Several regulations have been implemented to protect the ports. They include but are not restricted to (i) the Security Council Resolution 1373(2001)—United Nations, September 28, 2001; (ii) the International Maritime Organization (IMO) Resolution A. 924(22), the measures and actions for prevailing terrorist attacks (November 2001); and (iii) the Safety Of Life At Sea (SOLAS) Conference 5/34 Resolution 1 on December 12, 2002.

A number of studies have been conducted, revealing different aspects of transportation related to security perceptions. Jenkins and Gersten (2001) observed that passengers are alternatively sensitive to privacy and the severity of terrorism and threat, while Leo and Lawler (2007) found that passengers from and to Tel Aviv

registered a heightened perception of security threat. Moreover, a survey that took place in Thailand's airport showed that 56% of participants took seriously security into account when they were called to make a mode choice, especially in international trips (Udomsuk et al. 2006).

In the same perspective, Srinivasan et al. (2006) remarked that individuals bearing positive impressions about security measures were more likely to fly but that the utility of air mode decreased as security controls and boarding time increased. Elias et al. (2010) found that the individuals' fear and risk perceptions play an important role on the mode choice, while the perceived transport threat differs significantly depending on whether it is experienced by a woman or a man. The latter remark was also made earlier by Udomsuk et al. (2006).

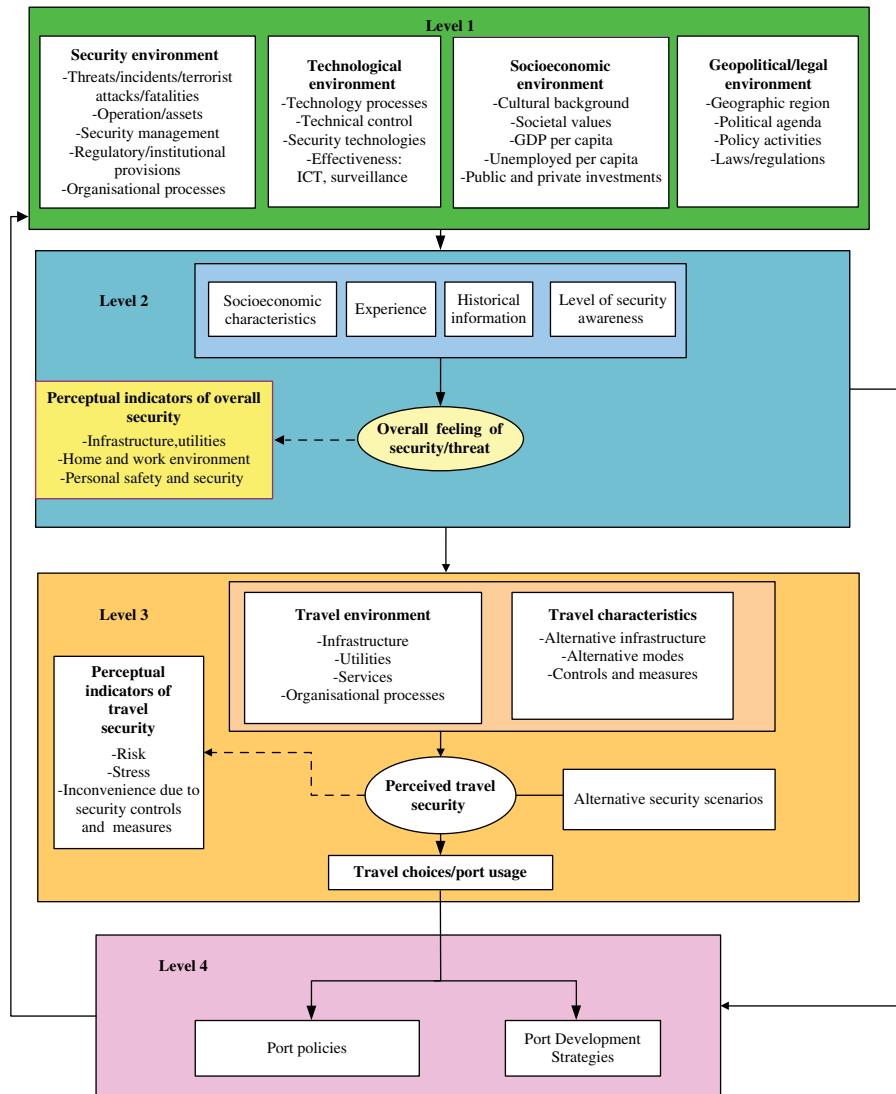
All research presented above, as well as the models that have been developed so far, focuses on two principal aspects of the field: (i) capturing the behavior of decision makers with regard to mode choice and (ii) reflecting transit usage under different security situations. An innovative aspect of the present research is its focus on the ports' passengers' behavior by analyzing port choices under different hypothetically stated preference (SP) scenarios. The foundations of this research lie on the work and findings of a related one pertaining to individuals' decision-making processes in a specific islander area (iPORTS project, funded by the EU Community Initiative Programme Interreg III B Archimed (2006)).

The present paper introduces a behavioral approach to model individuals' feelings and perceptions of security for the analysis of the impacts and effectiveness of security policies and measures at ports. Section 14.2 features the proposed methodological framework. In Section 14.3, a case study for port security at the island of Chios is presented and in Section 14.4 the model estimation and application results. Finally, Section 14.5 hosts the chapter's conclusions.

## 14.2 METHODOLOGICAL FRAMEWORK

The current research involves the development of a framework so as to understand, measure, and model the user's perceptions and feelings of security, use them to predict port usage, and subsequently evaluate alternative port policies and strategies. The framework in question is built on four levels, strongly interrelated (see Fig. 14.1). It is an extended framework based on the work of Ben-Akiva et al. (2002) and Litinas et al. (2010).

At *Level 1* takes place the understanding and identification of external factors affecting the development of all attitudes and perceptions formed by individuals and concerning their security and their respective choices. *Level 2* involves the determination of the process of the development of the overall feeling of security. This process is affected by individual-specific observable factors such as personal experiences, historical information on terrorist attacks, etc. *Level 3* focuses on the transportation industry, in the present case study on the port environment. At *Level 4*, alternative port security policies and port development strategies are designed. The models developed in Levels 2 and 3 are applied at the last level,



**FIGURE 14.1** Methodological framework.

where the impact of alternative security policies, strategic development measures, and scenarios is predicted.

The methodological framework presented here includes all the factors that affect the individuals' decision-making behavior, specifically the ones accounting for security attitudes and perceptions. Subsequently, a case study is developed to capture parts of the overall methodological framework and demonstrate its applicability and usefulness.

### 14.3 CASE STUDY: THE PORT OF CHIOS

This section presents a case study concerning the port of the island of Chios. The choice of the port of Chios for the case study can be attributed to the fact that, the construction of a new port being initially approved for funding, the local society became fairly interested in the development of the new port infrastructure. Therefore, the opportunity to provide survey participants with alternative SP scenarios regarding the redesign of the existing port for the implementation of security improvements was not to be overlooked.

#### 14.3.1 Data Collection

The data collected include revealed preferences (RP), SP, as well as attitudes and perceptions of the respondents. The questionnaire with which the collection was done included a wide range of SP scenarios aiming at capturing passengers' decision making toward port choice. Respondents were asked to choose between the old port and a new port under alternative scenarios. Three SP experiments were administered per respondent, where each port was represented in terms of a probability of terrorist attack and additional waiting time (in minutes) and travel cost (in euros) incurred in the transition from the current port to the new port due to the security improvement. Different levels of the above attributes were used in the SP experiments. The terrorist attack was described as a car loaded with explosives boarding on the ship (Table 14.1).

The data collection took place in the island of Chios, while the overall sample consisted of 200 individuals. Respondents were selected randomly and covered all socioeconomic classes.

#### 14.3.2 Security Attitudes and Perceptions

The present section presents the findings of the analysis of user's feelings/perceptions of security, following the different stages of the behavioral framework described in Section 14.2, that is, Level 1, external environment; Level 2, overall feeling of security; and Level 3, port specific feeling of security.

Since all questionnaires were answered at the geographic context of the island of Chios, all Level 1 characteristics are common. Levels 2 and 3 factors were identified by perceptual measurements (indicators) using 5-point Likert scales (Meyers et al. 2005).

**TABLE 14.1 Port Choice Stated Preference Scenarios**

	Current Port	New Port
Probability of terrorist attack (%)	0/25/50/75/100	0/25/50/75/100
Additional travel cost (€)	0/5/ 15/ 20	0/10/25/35
Additional waiting time (min)	0/1/ 10 / 5	0/5/ 1 5/ 10

**14.3.2.1 Level 2: Overall Feeling of Security** The respondents' impressions concerning a terrorist attack at a Greek port or airport is that of a high probability event. Somehow they still feel quite secure inside public transport modes and public places although they sometimes feel threatened when using the former.

**14.3.2.2 Level 3: Port Specific Feeling of Security** Overall, passengers seem to be quite satisfied with the current security measures in ports. More specifically, they declared being *quite satisfied* with passenger and luggage check before boarding, but being *moderately satisfied* with car check prior to boarding on the ship. In addition, individuals believe that higher levels of security would be extremely time consuming and would cause them discomfort. Furthermore, respondents believe that the construction of a new port and the adoption of suitable technological equipment are necessary when applying new security measures.

## 14.4 A PORT CHOICE MODEL

This section present a model developed for measuring the effect of security on port choices. It corresponds to Level 3 of the methodological framework. A total of 545 SP port choices were furnished with comprehensive information and used in the modeling effort.

### 14.4.1 Model Specification

A binary logit model was developed where the dependent variable is the choice between the current port and a new port. The new port is presented as more advanced technologically and with significantly higher security level. The main assumption is that an individual will choose the alternative with the highest utility (Ben-Akiva and Lerman 1985). For respondent  $n$  provided with a choice pair  $j$ ,

$$p_{nj}(1) = \frac{1}{1 + \exp(-\mu V_{nj})} \quad (14.1)$$

$$\begin{aligned} V_{nj} = & (\text{time}_{1j} - \text{time}_{2j}) \times \left( \alpha_0 + \sum_l \alpha_l \delta_{nl} \right) + (\text{threat}_{1j} - \text{threat}_{2j}) \times \left( \beta_0 + \sum_k \beta_k \delta_{nk} \right) \\ & + (\text{cost}_{1j} - \text{cost}_{2j}) \times \left( \gamma_0 + \sum_m \gamma_m \delta_{nm} \right) \end{aligned} \quad (14.2)$$

where:

- $P_{nj}(1), P_{nj}(2)$ : probability of choosing current port 1 and new port 2 given choice pair  $j$
- $\text{cost}_{1j}, \text{cost}_{2j}$ : travel costs of alternatives 1 and 2 given choice pair  $j$
- $\text{time}_{1j}, \text{time}_{2j}$ : waiting time of alternatives 1 and 2 given choice pair  $j$

- $\text{threat}_{1j}, \text{threat}_{2j}$ : probability of terrorist attack of alternatives 1 and 2 given choice pair  $j$
- $\alpha_0, \beta_0, \gamma_0$ : main time, cost, and probability of threat coefficients for all  $n$
- $\alpha_l, \beta_k, \gamma_m$ : additional time, additional impact of threat, and additional cost coefficients, which measure the effect of time, probability of threat, and cost for members of segments  $l, k$ , and  $m$ , respectively
- $\delta_{nl}, \delta_{nk}, \delta_{nm}$ : dummy (0/1) variables indicating membership in segments  $l, k$ , and  $m$ , respectively
- $\mu$ : the logit scale parameter, normalized to 1

#### 14.4.2 Model Estimation Results

Table 14.2 presents the estimation results of a mixed binary logit model. The model was estimated using the BIOGEME software (Bierlaire 2008) and takes into account repeated observations from the same individual. The coefficients included in the model are statistically significant and intuitively correct. The main attributes such as additional waiting time and additional travel cost have negative signs as expected, showing that people are neither willing to pay nor to wait more for higher level of security. Moreover, if individuals are satisfied with the current security measures,

TABLE 14.2 Discrete Choice Model Estimation Results.

Coefficients	Mixed Binary Logit Model	
	Coefficient Estimates	t-Test
$\alpha_{0\text{time}}$ : travel time difference in minutes $(\text{time}_{1j} - \text{time}_{2j})$	-0.153	-3.51
$\alpha_{1\text{time}} \times \delta_{n=1}$ : where $\delta_{n1} = 1$ if the respondent is male; 0 otherwise	-0.0786	-1.76
$\beta_{1\text{threat}}$ : difference in the probability of terrorist attack level ( $\text{threat}_{1j} - \text{threat}_{2j}$ )	-0.0107	-2.06
$\beta_{1\text{threat}} \times \delta_{n=1}$ : where $\delta_{n1} = 1$ if the respondent travels more than seven times per year; 0 otherwise	-0.0177	-2.25
$\gamma_{0\text{cost}}$ : travel cost difference in euros ( $\text{cost}_{1j} - \text{cost}_{0j}$ )	-0.0476	-2.41
$\gamma_{1\text{cost}} \times \delta_{nm=1}$ : where $\delta_{n1} = 1$ if the respondent believes that the construction of the new port and the introduction of suitable technological equipment are necessary for applying new security measures; 0 otherwise	0.0204	1.98
$\gamma_{2\text{cost}} \times \delta_{nm=2}$ : where $\delta_{n2} = 1$ if the respondent is satisfied with the current measures; 0 otherwise	-0.0128	-1.92
$\Sigma\text{Panel}$ – panel data sigma distribution (mean zero)	0.888	3.09
<i>Statistics</i>		
Number of observations	448	
Initial log-likelihood	-310.530	
Final log-likelihood	-245.937	
Rho-square	0.208	
Adjusted rho-square	0.182	

they are less willing to pay additional costs for a more secured port, as indicated by the combined coefficient of cost and satisfaction with the current security measures. On the other hand, individuals seem to be less reluctant to pay additional costs for switching to a more secured port, if they believe that the construction of the new port and the introduction of suitable technological equipment are necessary. The coefficient sign of the probability of terrorist attack is negative, indicating that the highest the probability of a terrorist attack in the old port, the highest the respondents' likelihood of choosing the new port.

Moreover, as it can be seen from the sign of the combined time and gender coefficient, men are less willing to cope with increased waiting times and therefore more likely to switch ports when the waiting time increases. In addition, frequent travelers (via ports) are more prone to switch ports when the probability of a terrorist attack increases, compared to those that travel less than six times per year. In this dataset, no additional socioeconomic coefficients related to the cost (such as income) were proven statistically significant; it is however believed that if a bigger sample is investigated, this would be the case. From the model estimation results, we can see that the sigma panel coefficient is significant, which means that the model allows for capturing intrinsic correlations among the observations of the same individual.

#### **14.4.3 Level 4: Willingness to Pay for More Secure Environment and Policy Implications**

When evaluating new measures, it is necessary to consider passengers' trade-offs between travel times/costs and security levels concerning travel-related decisions. The structure of the suggested model allows for the calculation of individuals' willingness to pay (WtP) for the use of an improved security-wise port. More specifically, assuming a linear relationship, WtP is calculated based on the ratio of two utility parameters,  $\beta_{\text{threat}}$  and  $\beta_{\text{cost}}$ , where  $\beta_{\text{threat}}$  represents the decreased probability of terrorist attack in the new port (security improved) and  $\beta_{\text{cost}}$  represents the ticket cost increase that will cover this security improvement:

$$\text{WtP} = \left( \frac{\beta_{\text{threat}}}{\beta_{\text{cost}}} \right) \quad (14.3)$$

Individuals are willing to pay as much as 22.5€ in excess of the initial ticket price (a 50% increase) to eliminate the probability of a terrorist attack and ensure a secure trip. In a similar vein, Potoglou et al. (2010) observed that the highest valuations in excess of the average price of a rail ticket in United Kingdom are 5.30€ (£4.44) and 4.26€ (£3.54) and they were justified by the efforts to increase the effectiveness of security authorities. Moreover, if in the WtP equation the coefficient for threat is replaced by the corresponding value for frequent travelers, the acceptable ticket price increases by 65.5%, meaning that the frequent travelers are willing to accept a price increase of as much as 37€ in order to eliminate the possible threat of a terrorist attack.

The suggested methodology, adopted by researchers and policy-makers, will prove immensely helpful for the design and validation of alternative security policies

(this corresponds to Level 4 of the methodological framework), since it allows for the identification and quantification of trade-offs between security measures and individual preferences. More specifically, the results can be used to assess the effectiveness of alternative policy options and design guidelines for EU and national policy formulation. They can also provide authorities and companies that conduct related research with sources of valuable information and recommendations on how to improve their performance.

## 14.5 CONCLUSIONS AND FURTHER RESEARCH

The present research illustrates the development of a methodological framework regarding passengers' perceptions and feelings of security at ports and the results from a case study for the port of Chios. The survey was conducted mainly by means of a questionnaire, a specific tool build to account for RP, attitudinal data, and SP scenarios. The descriptive analysis show that the general impression of people is that they are safe but that they are less than satisfied with both the personal and the car check carried out before boarding on a ship.

The SP scenarios reflected the port choices as a function of the probability of a terrorist attack in the next five years, an increased version of normal waiting time attributed to the introduction of additional security measures, and accordingly increased ticket costs. Despite the fact that in our study only age and trip frequency were found statistically significant, it is believed that more socioeconomic characteristics may prove to be so in a larger sample. The results also indicate that respondents are willing to pay for as well as to wait for security improvements. Overall, passengers are willing to pay as much as an extra one-third of their ticket price in exchange for the avoidance of a terrorist attack. However, they are less willing to wait for the implementation of new security measures.

The reader should keep in mind that in the majority of small/regional islands, individuals do not have a choice between alternative ports. However, in the case of a terrorist attack, travelers could use the airport instead and vice versa.

The case study shows that the methodology is applicable and useful to policy-makers. Further research should focus on the effect of specific measures (such as security cameras, security personnel, etc.) on the individuals' WtP more for a service, as well as on the identification of market segments that are positively or negatively disposed toward security measures and how these segments react to different security scenarios.

## REFERENCES

- Ben-Akiva, M. and Lerman, S. (1985). *Discrete Choice Analysis: Theory and Application to Travel Demand*. MIT Press, Cambridge, MA.
- Ben-Akiva, M., Walker, J., Bernardino, A.T., Gopinath, D.A., Morikawa, T., and Polydoropoulou, A. (2002). "Integration of Choice and Latent Variable Models." In *Perpetual Motion: Travel Behaviour Research Opportunities and Application Challenges*. Editor: H. Mahmassani. Oxford, Elsevier Science Ltd., pp. 431–470.

- Bierlaire, M. (2008). An Introduction to BIOGEME Version 1.7, [biogeme.epfl.ch](http://biogeme.epfl.ch) (accessed February 20, 2015).
- Elias, W., Shiftan, Y., and Albert, G. (2010). "Travel Behavior in the Face of Surface Transportation Terror Threat: The Israeli Experience." In *Proceedings of World Conference on Transport Research*, July 11–15, 2010, Lisbon.
- Hardin, R. (2004). "Civil Liberties in the Era of Mass Terrorism." *The Journal of Ethics*, 8(1), 77–95.
- Ito, H. and Lee, D. (2005). "Assessing the Impact of the September 11 Terrorist Attacks on U.S. Airline Demand." *Journal of Economics and Business*, 57, 75–95.
- Jenkins, B.M. and Butterworth, B.R. (2007). "Selective Screening of Rail Passengers," MTI Report 06-07. San José, CA, Mineta Transportation Institute College of Business.
- Jenkins, B.M. and Gersten, L.N. (2001). "Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices." MTI Report 01-07. San José, CA, Mineta Transportation Institute College of Business.
- Leo, J. G. and Lawler, J. P. (2007) A Study of Passenger Perception and Sensitivity to Airport Backscatter X-Ray Technologies, *International Business and Economics Research Journal*, 6(7), 11–18.
- Litinas, N., Kapros, S., and Polydoropoulou, A. (2010). Change of Values and Transportation Needs: Towards a New Transportation Strategic Planning Methodology. In *Applied Transport Economics: A Management and Policy Perspective* Editors: Eddy Van de Voorde and Thierry Vanelslander. Antwerp, De Boeck Publishing. [http://hoger.deboeck.com/titres?id=80905\\_1](http://hoger.deboeck.com/titres?id=80905_1) (accessed March 8, 2015).
- Meyers, L.S., Guarino, A., and Gamst, G. (2005). *Applied Multivariate Research: Design and Interpretation*. Thousand Oaks, CA, Sage Publications, p. 20.
- Potoglou D., Robinson, N., Kim C.W., Burge, P., and Warnes, R. (2010). "Quantifying Trade-Offs Across Privacy, Liberty and Security: A Large Scale Stated Preferences Study on UK's National Rail Network." In *Proceedings of World Conference on Transport Research*, July 11–15, 2010, Lisbon.
- Srinivasan, S., Bhat, C.R., and Holguin-Veras, J. (2006). "An Empirical Analysis of the Impact of Security Perception on Intercity Mode Choice: A Panel Rank-Ordered Mixed Logit Model." *Journal of the Transportation Research Board*, 1942, 9–15.
- Udomsuk, I., Yuttikul, C., Ninsonti, N., Buaklin, N., Thumakul, P., Hadsakun, P., King, M., Mouton, K., and Ngamson, B. (2006). "Tourist Perceptions on the Effects of Terrorism on the Airline Industry." International Program in Hotel and Tourism Management, Siam University, *5th Asia Pacific Forum, "Threats and challenges to the Tourism Industry: Reform and Perform,"* September 20–22, 2006, Thailand.



---

# 15

---

## PIPELINE SECURITY

LUCA TALARICO<sup>1</sup>, KENNETH SÖRENSEN<sup>1</sup>, GENSERIK RENIERS<sup>1,2,3</sup>,  
AND JOHAN SPRINGAEL<sup>1</sup>

<sup>1</sup>*Department of Engineering Management, Faculty of Applied Economics,  
University of Antwerp, Antwerp, Belgium*

<sup>2</sup>*Safety Science Group, University of Technology Delft, Delft, The Netherlands*

<sup>3</sup>*Center for Corporate Sustainability (CEDON), HUB, KULeuven, Brussels, Belgium*

### 15.1 INTRODUCTION

Pipelines are frequently used as a cheap and safe transportation mode for liquid, gas, and solid goods that can cover long distances, sometimes going through several countries. On the whole, pipeline accidents cause a few annual fatalities compared to transportation modes of other products. According to the U.S. Department of Transportation (2013), hazardous liquid pipelines caused an average of 1.8 deaths per year from 2006 to 2010. During the same period, natural gas pipeline accidents generated an average of three deaths per year (Parfomak 2012). In general, pipeline accidents can be classified by their cause (Kuik and Bolt 2003). If the historical data collected by national agencies (European Gas Pipeline Incident Data Group 2011) is analyzed, we can observe that in Europe and Canada the category of external interferences (which include intentional attacks) holds around 50% of the causes of accidents (European Commission 2011). According to Baker and Fessler (2008), the consequences of a pipeline accident can be divided into different categories, regardless the cause that engendered the disaster:

- *significant accidents* that generate damages greater than \$50,000 and produce either highly volatile releases or other liquid releases that might result in an unintentional fire or explosion;

- *serious accidents* that are a subset of significant accidents, including fatalities or injuries that require hospitalization.

Although pipeline accidents have caused relatively few fatalities in absolute numbers, a single pipeline accident can be catastrophic in terms of deaths and environmental damages resulting in serious contamination of marine, aerial, and terrestrial fauna and flora. For instance, in July 2010, the explosion of two oil pipelines in the port of Dalian, China, caused an ecological disaster on an enormous scale. More than 1500 t of oil was released into the Yellow Sea (Boston.com 2010). Furthermore, pipeline accidents could potentially affect other transportation modes or other critical infrastructures such as electric, military, and telecommunication facilities.

In this chapter, we expressly use the terms intentional deeds and malicious acts to denote actions intentionally performed by vandals, thieves, and (cyber) terrorists aimed at damaging pipeline transportation systems or pipeline support infrastructures such as supervisory control and data acquisition (SCADA) systems or attacks on electricity grids and communication networks (see, e.g., Shreeve 2006; Subramanian 2008). Intentional or malicious acts can generate even greater catastrophic damages to the national economies when they affect pipelines located in the so-called high-consequence areas, which include highly populated areas, commercially navigable waterways, water, and environmentally sensitive areas (e.g., drinking water supplies or ecological reserves).

The potential damage is also influenced by a number of factors such as the pipeline characteristics, the location of shutoff valves, the nature of the material transported through the pipeline, the topography of the pipeline route, and the time for the pipeline personnel or the emergency operators to be mobilized in case of accidents. All these factors are under the sphere of influence of pipeline operators, and they need to be adequately evaluated in order to take appropriate countermeasures to protect critical facilities from both intentional attacks (security-wise) and unintentional damages (safety-wise).

In the remainder of this chapter, we focus on the intentional attacks against pipelines and its consequences. In the first part, we classify intentional acts followed by an overview of the minimal information needed to secure pipeline infrastructure. In the second part, we describe the most common measures to prevent intentional acts and/or reduce their consequences. We conclude with a mathematical model that enables to choose the appropriate countermeasures to secure a pipeline system given a limited budget.

## 15.2 INTENTIONAL ACTS

Several definitions of “critical infrastructure” have been given during the last decades. The most complete definition is “... (set of) systems and (physical or virtual) assets so vital for a nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health

or safety..." (Department of Homeland Security 2003; The White House 2000). The effects of a terrorist attack to a critical pipeline infrastructure can spread far beyond the direct target and reverberate long after the immediate damage (U.S. Office of Homeland Security 2002).

The critical pipelines used to transport oil, gas, and hazardous liquids represent a viable target for intentional acts such as vandalism, sabotage, or even a terrorist attack. In wartimes, for instance, pipelines are often the target of military attacks since their destruction can seriously disrupt the logistics of the enemy. For example, the attacks against oil and gas pipelines in Iraq have been extensively adopted as a war tactic against the US army. Between 2003 and 2008, an average of 10 terrorist attacks per month occurred, despite the major efforts by the US security forces to ensure their unimpeded operation (Institute for the Analysis of Global Security (IAGS) 2008). In Colombia, the terrorist groups FARC and ELN, which are at war against the government since 1964, have attacked the national pipeline Caño Limón–Coveñas so many times over the past 5 years that it has become known as the *flute* (IAGS 2013). During the most recent of these terrorist attacks occurred in July 2013, the second biggest Colombian oil pipeline was shut down (Reuters 2013).

Intentional acts from third parties can be classified into three main categories depending on the purpose of the attack: *vandalism and sabotage*, *terrorism*, and *cyberattack*.

### 15.2.1 Vandalism and Sabotage

Vandalism and sabotage are closely related terms, their main purpose not being to create environmental damages or to spread terror among the population, but to intentionally disrupt pipeline operations either for personal interests (vandalism) or for protests (sabotage).

Vandalism against pipelines refers to illegal or unauthorized activities that involve the destruction of pipelines to interrupt the material supply or the puncturing of pipelines to siphon the transported materials (e.g., crude oil or its related products) so as to exploit them for personal use or to sell them on the black market (Onuoha 2007). This activity sometimes ends tragically. For example, in 1998, more than 1000 villagers in Nigeria died while scavenging for fuel when a ruptured gasoline pipeline exploded (Luft 2005). It is estimated that 15% of Nigeria's production capacity, which accounts for 3.1 million barrels/day, normally remains unavailable because of recurrent acts of vandalism.

Sabotage acts can be performed by single individuals, groups of persons being members of the same organization/association, or even nations aimed at intentionally damaging pipeline operations. The reasons behind the act of sabotage are not purely economic; they may also have a political, social, or environmental nature. Secondary motivations include (Muhlbauer 2004):

- an indirect attack against a government that supports the pipeline;
- a means of drawing attention to an unrelated cause;

- a protest for political, social, or environmental reasons;
- a way to demoralize the public by undermining public confidence in its government's ability to provide basic services and security.

Repeated acts of pipeline sabotage, from 2003 to 2005, in Iraq determined more than \$10 billion in lost oil revenues (Luft 2005). In September 2007, six simultaneous attacks by saboteurs from the people's revolutionary army (EPR) group against oil and gas pipelines caused severe supply shortages in Mexico, leading to the temporary closure of several factories (Hernandez 2007). In 2012, the attacks carried out by the rebel groups FARC and ELN in Colombia kept the government far from reaching its target of 1 million barrels/day. Baluchi insurgents in Pakistan are particularly fond of attacking the gas pipeline in Dera Bugti because they estimate that the pipeline operator exploits their resources without a reasonable compensation (Khan 2006).

Vandalism and sabotage represent potential threats that require close attention when the pipeline is in an area of political instability or public unrest (Baran 2007). In Steinhäusler et al. (2009), a model has been developed to define the spatial characteristics of the most probable sabotage sites in relation to the sociopolitical conditions surrounding the pipeline. In this research, the pipeline network Baku–Tbilisi–Ceyhan (BTC), which passes through Azerbaijan (278 miles), Georgia (153 miles), and Turkey (668 miles), has been studied. The BTC is a possible target of different sabotage acts from different terrorist groups due to the ongoing Russian–Georgian crisis. For security reasons, the BTC runs along its entire length underground. As a consequence, the most vulnerable points along the pipeline are related to the infrastructures above the ground such as block valve stations, check valve stations, pumping stations, and oil terminals. The results of the study demonstrate that the most vulnerable BTC sections that could attract future acts of sabotage are those that present:

- proximity to current conflict areas or possible problematic areas in the future;
- low transportation network density;
- low population density or relatively remote areas where activists cannot be observed, for example, when digging to set up the explosives;
- low relief values;
- land cover dominated by different kinds of forests (mixed, deciduous, evergreen) and or agricultural fields that allow the saboteurs to move from one place to another unobserved;
- proximity to ethnic homeland areas, since the saboteurs would found logistics support and a safe retreat in case of attacks.

### 15.2.2 Terrorism

Before September 11, 2001, the pipeline industry had been concerned primarily with environmental, safety, and maintenance issues. Apart from occasional episodes of vandalism, intentional acts were hardly perceived as a serious threat to the world's

pipelines' infrastructures, even though they have always been used to carry roughly half of the world's oil and most of its natural gas. With the threat of terrorism looming, pipeline operators in the industrialized world have taken action to prevent international terrorism from targeting their infrastructures. Terrorists can be defined as "nonstate armed actors" and can be divided into (Farah 2012):

- terrorist groups motivated by religion, political activists, or ethnic forces;
- transnational criminal organizations, both structured and disaggregated;
- militias that control "black hole" or "stateless" sectors of one or more national territories;
- insurgencies, which have more well-defined and specific political aims within a particular national territory but may operate from outside of that national territory.

Attacks on oil and gas installations have become the weapon of choice for international terrorism, irrespective of the political system and social–financial boundary conditions of the society under attack (Steinhäusler et al. 2008). It is worth mentioning few examples: from 2011 to 2013, Jordan's natural gas supply was interrupted 16 times due to several terroristic attacks on the pipeline segments located in the Egypt's Sinai Peninsula (Ya'ar 2013); in 2004, Chechen terrorists were able to blow up several pipelines around Moscow, Volgograd, Dagestan, and Stavropol despite the increased security efforts of the Russian security forces (Kupchinsky 2005); and in 2006, the Indian terrorist group ULFA staged several pipeline attacks in the oil-rich region of Assam (Luft 2005). According to Makarenko (2003), terrorist threats against the pipeline industry can be classified into the following categories ordered by their frequency of happening:

- pipeline bombing (causing an explosion of the pipeline);
- kidnappings of pipeline company personnel;
- hijacking of energy installations accompanied by the taking of hostages;
- direct armed attacks on pipeline company personnel;
- attacks on depots;
- attacks on corporate offices of pipeline companies;
- other sabotage acts such as the contamination of the material transported by the pipelines.

Among all categories of terrorist threats, pipeline bombing is the most common one, especially if the transported material is gas or oil. A list of 49 major accidents happened from 2004 to 2012 can be found in Taylor (2012). These accidents involve gas and oil pipelines all over the world and are clearly ascribed to terroristic organizations (such as Al-Qaeda, Al-Shabaab, ex-Gitmo detainees, and the Pakistani Taliban). This list does not include pipeline accidents due to vandalism, sabotage, or war-strategy acts registered in instable countries (e.g., Iraq). In Table 15.1, a geographical distribution

**TABLE 15.1 Geographical Distribution of Terroristic Attacks to Oil Pipelines**

Geographical Area	% of Oil and Gas Terror-Related Accidents (2004–2012)
Africa	10
Asia	12
Europe	6
South America	6
Middle East	20
United States and Canada	45

Adapted from Taylor (2012).

of these terrorist attacks is presented. In January 2011, a report from the US Department of Homeland Security entitled “TSA Liquid and Natural Gas Pipeline Threat Assessment 2011” registered 44 suspicious pipelines and related oil and natural gas activities from January 2010 to October 2010. Suspicious activities near pipelines may indicate an interest to collect information for a future attack or the desire to identify vulnerabilities or test a pipeline facility’s security and response operations.

An analysis conducted by Simonoff et al. (2005) indicates that during the period 2000–2005, the number of attacks on gas and oil facilities has increased in countries where Islamic terrorist groups operate. In general, attacks on the gas and oil sector present a relatively small proportion of total terrorist attacks (less than 1%). According to Rapier (2010), between 2005 and 2010, attacks to oil pipelines executed by international terrorist organizations have significantly diminished. This decrease could have been triggered by two main factors. On the one hand, the protection of pipelines has become a high priority among the majority of oil-producing and oil-consuming nations. As a result, the increasing investments in their security might have made the attacks to pipelines too difficult for the terrorist cells, which do not have the financial means to bypass advanced security measures. On the other hand, terrorists choose their own target on the basis of what is of interest for the media. The destruction of remote pipelines may not be reported by the international press, while other targets such as civilians ensure a higher media coverage. Therefore, terrorists with the objective of making a statement to the world probably would not act without having their activities reported. Actually, terrorist attacks are targeted at critical pipelines and facilities, suggesting that terrorists pick up their targets for strategic reasons (McDermott 2004). The targets are usually selected in order to maximize the consequences of the damages. According to the data, the most common components targeted are pipelines (69.5%) and production facilities (15.1%). This is significant in revealing what modes and locations tend to be easier to attack. In general, attackers prefer pipelines that run aboveground, but transmission lines and their pylons are also targeted.

In general, the targets are revenue-generating facilities, and their destruction determines not only the interruption of the flow of materials but also the related cash flow. According to the American Petroleum Institute, the pipeline industry is subject to terrorist attacks due to the following two factors:

- The physical and chemical properties of the transported material may cause a malicious release with the intent to harm a neighboring population.
- The critical importance of the products supplied by pipeline operators may determine the disruption of operations of the whole industry.

In 2012, the US National Intelligence has stated that on a global scale, major pipeline security problems are located in the following geographical areas:

- *Middle East*: This area holds between two-thirds and three-quarters of all known oil reserves (Telhami 2002). This politically volatile region also hosts the world's largest oil processing plant (Abqaiq) with a capacity of up to 6.8 million barrels/day. A successful terrorist attack disrupting operations for an extended period of time would have global repercussions.
- *Africa*: The northern part of the continent has been engulfed by the Arab Spring social revolutions, which are gradually creating the potential for world instability resulting in an increase of global terrorism. The probability that future activities of terrorist groups (e.g., Armed Islamic Group) will target pipeline installations (e.g., Trans-Saharan gas pipeline and West African gas pipeline) is a growing threat. Moreover, in Niger, the local movement for the emancipation of the Niger delta, backed up by large segments of the population, is likely to continue its repeated attacks on oil and gas installations in the exploration area of the delta in the form of pipeline rupture, kidnappings, and sabotaging oil fields (Steinhäusler et al. 2008). In August 2012, the West African gas pipeline was destroyed when pirates who had tried to board an oil tanker damaged severely the pipeline with their anchor. For over 2 months, the supply of gas to Ghana, Togo, and Benin caused major power supply problems to the affected countries (Gasol PLC 2012).
- *Central Asia*: The BTC pipeline is at risk from regional insurgents and members of Al-Qaeda who are reportedly planning acts of sabotage. The Kazakhstan–Xinjiang pipeline is facing increasing terrorist attacks by hostile Muslim Uighur minorities. The Southeast Turkey pipeline is threatened by a bomb attack campaign carried out by guerrillas belonging to the Kurdistan Workers' Party (PKK). The Druzhba pipeline, extending over 4000 km, is the longest pipeline in the world and has a capacity of 1.2 million barrels/day. Its route runs through areas of high political volatility in the North Caucasus region of Russia. In view of its strategic importance for the energy supply of Ukraine and Germany, this pipeline represents a high-value target for terrorists (Steinhäusler et al. 2008).
- *Asia*: The growing demand for raw materials transported through pipelines (e.g., oil and natural gas) by different emerging global economies (e.g., China, India) might catch the attention of terrorist groups that are based in some Asiatic countries characterized by political instability (e.g., Afghanistan, Pakistan). Critical targets for terrorist attacks are the Central Asia–China gas pipeline, which crosses Turkmenistan, Uzbekistan, and Kazakhstan arriving to China,

and the Kazakhstan–China oil pipeline. Also, the Trans-Afghanistan pipeline, which crosses Turkmenistan, Afghanistan, Pakistan, and India, is continuously exposed to terrorist threats. An interruption in the energy and in the raw material supply might severely threaten several major industrial countries in the whole continent.

### 15.2.3 Cyberterrorism

In order to transport products through pipelines to intermediate facilities or to the final customer, several physical interconnections of pipeline sections might be required. Besides the physical connections, digital interconnections between pipeline systems are used to control and monitor in real time the state of physical pipelines that may belong to different operators and/or companies responsible for pipeline security. Hence, in order to have a complete view of the pipeline system, thus preventing the accidents and reducing the response time in case of attacks, digital interconnections between several ICT systems are required. Yet for all the advantages that digital interconnectivity offers, pipeline infrastructures are increasingly vulnerable to attacks from an array of cyber threats (U.S. Department of Homeland Security 2008).

Physical assets in pipeline networks include the material transported, pumps, separators, compressors, pipes, valves, etc. The computer and the communication links that control the flow of the material transported by the pipeline can be considered either physical or cyber assets, the latter including also data transmitted and stored on the computers and spread over the communication lines or the software used to process that data.

Cybersecurity typically entails protecting both physical and cyber assets from operational failure or manipulation due to unauthorized access to operating software or data. Securing critical infrastructures may require a broad combination of both physical and cyber measures (Moteff and Parfomak 2004). In general, pipeline operators monitor and control the state of the pipeline network using a SCADA system, which can be accessed through internet. In addition to a physical attack, terrorists may launch an electronic attack that could affect data, software, or equipment/process controls (e.g., damage a piece of equipment or cause a dangerous chemical release by opening or closing a valve using off-site access to the SCADA system). Terrorists may also use technical means to intercept radio or phone traffic (U.S. Department of Homeland Security 2005).

Cyberattacks against the SCADA system are aimed at stealing crucial information that could compromise security of the pipeline infrastructure itself (Clayton 2013). Cyber intrusions into the informatics system of pipeline organizations can be aimed at:

- using remote administration tools to collect sensitive information;
- gaining unauthorized access to confidential data;
- changing the state of the pipeline network performing unauthorized operations.

According to an investigation of the Office of Cybersecurity and Communications (2009), the number of documented attacks has been continuously increasing since 2005. Hackers

have increasingly managed to use the data to directly reset computer-controlled pipeline systems, sabotaging them through extreme pipeline pressures or unsafe valve settings that could result in explosions or other critical failures. The industry's most visible response to the threat of cyberterrorism has been a creation of coalition of pipeline operators that provides a near-real-time threat and warning capability to its members on a 24/7 basis. The Department of Homeland Security's ICS-CERT publicly revealed information on a series of attacks that targeted a gas compressor station, which is a key component in moving gas through pipelines network in the United States. On February 2, 2013, the ICS-CERT received a report from a gas compressor station owner about several attempts to access the process control network. The attacks were originally traced back to 10 IP addresses. Fortunately, none of the cyberattacks were successful, and they stopped after March 2013 (Lennon 2013).

### 15.3 INFORMATION MANAGEMENT FOR PIPELINE SECURITY

Pipeline operators can influence both the probability of a malicious attack happening and the consequences of that event by correctly managing the information related to the pipelines under their supervision. Information management is crucial to have the right information properly stored, maintained, and updated. In this section, the minimal information that needs to be managed by pipeline operators is discussed.

#### 15.3.1 Physical Pipeline Characteristics

In general, pipelines can be very long and may cross several countries, regions, provinces, and cities, each with a different geopolitical situation. In such cases, it is obvious that a continuous monitoring of the status of the pipeline is a true challenge. Each pipeline operator should gather and store data concerning:

- *The general pipeline system:* It is important to have a general overview of all parts of the transmission line through which the materials are transported. Pipelines may be (partially) buried underground (e.g., in areas where saboteurs are known to operate) and (partially) aboveground. They may also be (partially) situated underwater. It is also important to have a detailed and updated map of all the possible interconnections with other pipeline networks (National Pipeline Mapping System 2012).
- *The pipeline segment:* Pipeline systems can be broken down into several homogeneous pipeline segments for two important reasons: (i) to represent a branch or an intersection with another pipeline segment and (ii) to allow for a change of associated features (e.g., diameter). Some features (e.g., the material transported) do not change for the entire pipeline system, while other features vary on a segment-specific basis. Each segment must be uniquely identified, and several features of each segment should be monitored, such as, isolation valve spacing, material, geographical location, operating parameters, soil corrosiveness, and leak history (The American Society of Mechanical Engineers 2004).

The use of different materials for each pipeline segment (e.g., protected and unprotected bare steel, plastic, concrete) implies different purchasing costs, maintenance, lifetime, integrity issues, compatibility with materials transported, etc. Moreover, the material used for the pipeline has an impact in terms of security. An example of decision taken by the pipeline operators to protect a whole pipeline network from terrorist attacks is the BTC pipeline network. It is buried for most of its 1700km and runs through more politically stable countries which are less exposed to security threats. These measures drove up the costs for this project to 3.6 billion US dollars, which is probably excessive given the fact that the pipeline's susceptibility to terrorist attack is limited. However, major pipeline projects in the future could be modeled on the BTC (Johnston 2008). Some modern technologies use sensors (see Section 15.3 for more details) applied directly around the pipeline in order to detect anomalies like an adversary attempting to damage the pipeline's external surface. The data gathered by sensors are sent to a central office, where every anomaly is detected and analyzed.

### 15.3.2 Product Transported through Pipelines

Many pipelines carry volatile, flammable, or toxic materials that could potentially engender public injuries and environmental damages. It has been estimated that in 2007 the total length of high-pressure transmission pipelines around the world is equal to 3,500,000 km. On average, 64% of the high-pressure pipeline infrastructure is used to carry natural gas, 19% petroleum products, and 17% crude oil. These systems are vulnerable to intentional accidents and terrorist attacks. The transported material and its operating conditions (e.g., pressure, temperature, density, volume) are both crucial to determine the criticality of the pipeline infrastructure. In general, a classification of the products that are being transported is based on the following substance parameters: state (e.g., liquid, gas, solid), hazardousness, flammability, toxicity, contamination capacity, and operating pressure.

The consequences of an attack may differ depending on the characteristics of the material. The pipeline operator should therefore define the level of criticality of the infrastructure by evaluating the possible disaster scenarios (e.g., explosions, toxic cloud migrations, thermal radiation effects, toxic releases) that can arise after an attack. Adequate countermeasures should be adopted depending on the criticality of the infrastructure.

### 15.3.3 Geopolitical Information

Geopolitical conditions in which the pipeline is located represent for each operator an important source of information that allows to establish the potential threats to which the pipeline infrastructure is exposed. Many pipelines are located in remote areas or underwater where no communication exists. Although surveillance and physical protection systems can be adopted, they are more onerous than they might

be if pipelines were located in more accessible areas. In general, the geopolitical factors, which affect directly the criticality of the pipeline, comprise:

- *Geological conditions*: The geological characteristics of the ground (or the seabed if the pipeline is underwater). Several geographical locations such as deserts, polar areas, or the ocean floor can present difficult access conditions for inspection and monitoring and can entail long response times in case of accidents.
- *Class location*: The level of human population within a certain distance on either side of the pipeline, which may be involved in case of accident.
- *Depth of the pipeline*: If the pipeline is located underground, it is important to know if a possible leak can contaminate the groundwater.
- *Weather conditions*: For some materials like beverages, a variation in temperature or humidity conditions could increase the risk of bacterial proliferation. Other meteorological conditions (e.g., atmospheric turbulences and wind speed) may interfere with the security infrastructures by creating nuisances to the sensors used to detect intrusions in the pipeline perimeter.
- *Political situation*: In geographical areas in which the political situation is not stable, conflicts or wars can occur, exposing pipeline segments to vandalism, sabotage, or terroristic attacks (Cohen 2006). Moreover, pipelines used to transport energy resources (e.g., oil and natural gas) are not merely an element of trade. They influence geopolitics and international security issues as well. For example, at the beginning of 2009, a dispute between Russia and Ukraine led to a major political crisis, affecting several European Union countries heavily dependent on Russian gas (Chow et al. 2010).

#### 15.3.4 Data and Information Sources

The data and the information related to the current state of the pipeline system are crucial for the pipeline operators. In this section, we examine the different available sources of information, the frequency at which the data should be gathered, and how the information can be stored.

Once the pipeline operator knows the minimal data and information required to execute a security risk analysis, the correct information needs to be found, preferably with minimal efforts. The data can be obtained from a wide spectrum of internal (i.e., within the operating company) and/or external (e.g., industry-wide data) sources. In many cases, the specific documentation containing the attributes of each pipeline segment is located within the operating company such as the design and construction documentation; current operational, inspection, and maintenance records; existing management information system; prior risk or threat assessments results; and internal personnel expertise. Valuable data can also be obtained from external sources such as geographic information system (GIS) databases; experts involved in the risk assessment and integrity management program processes; jurisdictional agency reports and databases; and industry consortia, research organizations, and other operators.

Pipeline systems and the environment in which they operate are rarely static. This peculiarity makes the pipeline security risk assessment and management a never-ending process. Each pipeline operator should therefore adopt a systematic process to monitor all the pipeline's internal (e.g., system design, operating conditions, and maintenance) and external changes (e.g., the environment in which the pipeline operates). In fact, such changes can modify the exposure of the pipeline to external attacks, the probability to be attacked, and/or the consequences in case of accidents (e.g., after a change in the operating pressure). A war or a political instability in a specific region traversed by a pipeline infrastructure can drastically increase the risk of sabotage, and thus, stronger protections and adequate security measures should be adopted in such a situation. A change in the design of the infrastructure (e.g., a pipeline segment that needs to be located aboveground) can expose the pipeline to terrorists or saboteurs and should be accompanied by the necessity to have additional protection.

Each operator is required to assess the integrity of the pipeline periodically. For instance, anomalies in the geometry of the pipeline segments and corrosion phenomena can expose a segment to a higher probability to be drilled by vandals or saboteurs. Also, the status of the security system (e.g., fences, sensors, cameras) used to protect the pipeline's infrastructures needs to be verified in order to maintain its efficacy to prevent attacks. The interval for assessments depends on the pipeline system, for example, on the risk in case of attack. Sometimes, these intervals are defined by jurisdictional institutions.

In general, a single (digital) repository containing data gathered from both internal and external sources helps to improve the quality, the quantity, and the timeliness of information. Nowadays, pipeline operators have to interact with hundreds of suppliers, partners, and institutions in order to increase their flexibility and reduce operating cost. In such a scenario, instead of maintaining a single shared central data repository updated in real time, thanks to technology, it is possible to set up a distributed database in which each pipeline operator can integrate its internal information and combine it with the information stored in other locations such as partner databases, jurisdictional databases, provider databases, and so forth. Issues related to data access authorizations and level of permissions should be properly addressed and managed in order to reduce cyberattacks or access violations to confidential data. Additionally, since data are gathered by merging and utilizing multiple data sources, consistency should be preserved.

### 15.3.5 Open versus Confidential Information

On the whole, the information required by each operator to prevent and protect the pipeline infrastructures can be classified as follows:

- *Public*: The information is in the public domain and freely accessible.
- *Confidential*: The information is confidential but can be shared with national agencies or study groups often treated in anonymous form.
- *Reserved*: The information remains inside the company and cannot be spread outside unless agencies or institutions expressly require so.

Public domain information is important for public awareness in case of safety-related accidents such as location of the pipeline (e.g., buried, aboveground, underground) and material transported. Confidential and reserved information is nonpublic. It includes:

- personnel engaged in the pipeline infrastructure;
- ICT infrastructure including password and permission;
- critical characteristic of the infrastructure (such as position of the main valves);
- pipeline protection and security facilities;
- inspection–maintenance, vulnerability, security, emergency, and recovery plans.

Due to the sensitivity of reserved information, pipeline operators should adopt all the countermeasures necessary to maintain the confidentiality of such information, such as (Transportation Sector Network Management 2006) the following:

- limit the number of people with access to confidential information;
- store confidential documents in safe locations by using secure access codes;
- ensure that electronic versions of confidential documents are properly password protected and/or stored in servers/drives where access can be controlled.

#### **15.4 SECURITY COUNTERMEASURES**

Terrorists have demonstrated the ability to finance, plan, and carry out complex and sophisticated attacks against multiple targets over extended periods of time and in multiple locations (U.S. Department of Homeland Security 2005). Terrorist attacks can come from any direction along the pipeline system, at any time, in any manner. Since not everything can be protected, it is necessary to focus on the protection of critical pipeline segments.

Pipeline operators have to determine possible threats and for each of them adopt appropriate countermeasures depending on the materials transported, the pipeline characteristics, and the environment in which the pipeline is located. Countermeasures should also prioritize high consequence areas. In order to reduce the likelihood of a terrorist attack, some analytical steps need to be performed:

- Evaluate the “attractiveness” of a pipeline system or a pipeline segment.
- Risk profiling of the geographical area crossed by the pipeline to be protected. It is important to explore the areas surrounding the critical segment by locating buildings or facilities, which can become potential hiding spots for attackers. Moreover, it is important to have a deep knowledge of the geographical conformation of the interested areas (e.g., presence of hills, undulations, or flat area) and the weather conditions (e.g., strong winds or snow).
- Define the types of attackers that may target the pipeline segment, for example, vandals, thieves, trespassers, and terrorists.

Once the preliminary screening has been performed, appropriate measures need to be studied, taking into account the security budget and the characteristics of each solution (see Section 15.4 for a detailed decision model). When evaluating the available technologies, the major requirements should be:

- system durability/reliability;
- minimal nuisance alarms;
- maximum detection capability;
- ease of use and understanding;
- ability to quickly and accurately pinpoint the location of intrusion;
- ability to work with other existing and often complementary technologies;
- installation cost and maintenance.

The capability of each security countermeasure to detect potential threats can be evaluated using the index to quantify the quality of the performance (QOP) described in Owen (2013) according to the following formula:

$$\text{Quality of performance (QOP)} = \text{detection rate} \times \% \text{ confidence}$$

where

$$\text{Detection rate} = \frac{\text{number of detects}}{\text{number of tests}}$$

and

$$\% \text{ Confidence} = \frac{\text{number of hits}}{\text{number of alarms received}} \times 100$$

The QOP is used as a measure of the effectiveness of a countermeasure. The higher QOP, the higher the number of threats that the countermeasure is able to detect.

Measures generally adopted to prevent third-party attacks can be classified as follows: **traditional countermeasures**, which include *lighting, fences, access controls, deployment of security personnel, aerial surveillance, and ground patrolling*, and **advanced countermeasures**, such as *open-air intrusion detection sensors, not open-air sensors, remote sensing systems, and drones*. In general, all these measures belong to the category of the perimeter security system that attempts to prevent intruders from reaching their target.

Additional prevention measures can be adopted by pipeline operators such as:

- *Hiring personnel*—pipeline operators should adopt strict policies and alert mechanisms in case of hiring suspicious personnel (e.g., looking out for a spy

or an infiltrated terrorist). These measures according to the Transportation Sector Network Management (2006) include:

- Establishing policies and procedures for the applicants' preemployment screening and behavioral criteria for disqualification of potential candidates and employees;
- Carrying out preemployment background investigations of applicants for positions that are assigned to security roles;
- Verifying that contractors have background investigation policies and procedures at least as rigorous as the pipeline operators;
- Carrying out recurring background investigations on a regular basis for employees who work in security positions or who have access to sensitive information/areas;
- *Training the personnel*, which should have the technical skills and the knowledge to face different scenarios (e.g., terrorist attack, evacuation after disaster, kidnapping).

Other measures to be adopted include the usage of certain pipeline isolation valves at block valve sites or other aboveground installations in order to initiate a total shutdown, reduce partially or totally the operating pressure, and start some temporary action of repairing. It is worth noticing that valves may be operated remotely by signals from the pipeline control room. In other cases, the site may need to be visited for manual valve operation.

Additional security measures that can be adopted to prevent and protect any intentional leak to high-pressure transmission pipelines concern strategic choices on the physical pipeline infrastructure. For instance, coating can be applied to the pipeline surface so as to protect and fortify this surface from holes and drills. However, this protection measure is useless if attackers use weapons, bombs, etc. (Matheson and Cooper 2004). In this case, the only way to mitigate the damage is to interrupt the flow of the liquid/gas going through the pipeline. The fortification of pipelines via the new coating technologies, such as external carbon fiber wrap, can partially mitigate the effects of explosive devices. Similarly, it is important to shorten the lead time between the attack and reparation. The quicker it takes to repair the damage, the lower the cost of the disruption. Pipelines' saboteurs often target critical junctions or hit parts that it takes longer to replace. In order to reduce the lead time, pipeline operators should also maintain sufficient inventories of spare parts (Luft 2005).

#### **15.4.1 Perimeter Protection Measures**

Perimeter protection measures are security countermeasures that are commonly adopted by pipeline operators due to their suitable cost-effectiveness ratio. As formerly stated, the effectiveness of these countermeasures can be measured by pipeline operators using several standards (e.g., QOP described before) or customized measures. Undoubtedly, the effectiveness depends on the pipeline's characteristics and its geographical position.

The role of any perimeter security system is to act as the first level of site protection. This system defines the boundaries of the site and works as an early warning of intrusion attempts. Outdoor perimeter protection follows the fundamental security rules known as the five Ds: *define, deter, detect, delay, and detain* any intrusion into the protected area.

Perimeter protection needs to be tailored to suit the specific requirements of each site. Site layouts, sensitive areas, facility buildings, the surrounding environment, local weather conditions, and topography are all factors that need to be considered when planning a perimeter intrusion detection system. These parameters influence the selection of the detection technologies and the subsequent overall system performance. Even the very best sensors will deliver less than optimum performance if not correctly tailored to meet the site requirements.

Often, the final intrusion detection solution will consist of several different but complementary technologies to form “rings of protection” according to a multilayered approach against known and perceived threats. The more layers or obstacles an intruder needs to get through to reach his target, the more determined he will need to be. The more likely he will be detected, and therefore the more secure the site.

#### 15.4.1.1 Traditional Countermeasures

**Lighting:** Effective perimeter protection begins with a good fence and adequate lighting. Lighting can be a useful low-cost deterrent to potential intruders by providing improved surveillance and observation of suspect activities. However, the most determined criminals will not be discouraged by reaching their target. Therefore, multilayer security systems are needed where lighting forms represent an integral part. Undoubtedly, very often, it is not possible to use lighting for an entire pipeline network due to economic restrictions. Without considering the maintenance and installation costs (which represent a minor investment in comparison with the operating cost), the energy required to enlighten 150 m of fence varies from 150 to 4000 Wh. This quantity depends on the characteristics of the lighting system used (e.g., floodlights mounted on tall poles or LED mounted on the fence itself) and the distances between two consecutive light spots.

**Fences:** The cheapest way to protect an existing pipeline is to prevent easy access by surrounding it with walls and/or fences. Solid walls, as attractive as it sounds, may provide concealment opportunities for an intruder. Fences often allow for unobstructed observation of an intruder, and therefore, they may represent a deterrent for those attempting to enter illegally into pipeline perimeters. However, since using fences to protect all the length of the pipeline will be unrealistic from a financial viewpoint, pipeline operators usually use fences to protect critical segments of the pipeline and vulnerable assets such as valves and pressure pumps that can be used to block the flow of gas or liquid inside the pipeline after an attack. In general, in order to have a clear observation through fences, they should have adequate lighting and be devoid of vegetation from both sides. Hence, large trees and overhanging branches, which may provide climb points, should be removed. Besides defining the boundary of the site, the fence should also provide a sufficient

delay to an intruder climbing it to give the intrusion detection system enough time to activate and position cameras to visually verify the intrusion activity. Whenever vandals and trespassers represent the major threat, a chain link fence topped with barbed wire is probably adequate. On the contrary, if possible intruders are experienced thieves skilled and equipped to a higher level, then razor wire topped anti-climb prison-style fences need to be installed. The higher the fence, the more difficult it is to climb. A typical 2 m high fence is used for low-security areas, 3 m for medium-security areas, and 7 m for high-security sites. The average cost range of a basic fence goes from 10 to 50€/m depending on its height, its material, and the accessories (e.g., fiber-optic sensors, vibration sensors, acoustic sensors, microwave sensors) that can be attached to the fences so as to increase its efficacy (e.g., measured by the QOP index described before).

*Access Control:* Each pipeline operator should define policies in order to protect pipeline facilities from unauthorized access. In particular, physical security and access control measures need to be adopted to deter unauthorized vehicles and persons from entering the perimeter of the facility. If the level of criticality is low, the following basic procedures may suffice:

- Developing identification (ID) policies and procedures for employees and on-site personnel who have access to secure areas or sensitive information;
- Closing the secure doors, gate, and entrance when not in use;
- Using warning signals at regular intervals that are visible from any potential point of entry.

If the level of criticality is high, enhanced security measures need to be adopted (in addition to the basic measures) such as (Transport Security Administration 2011):

- Implementing procedures (e.g., manual and electronic sign in/out) to control the access to the facility locations;
- Monitoring visitors, contractors, and/or employees being at critical facilities;
- Establishing and documenting key control procedures for key tracking, collection, and loss;
- Using patent keys to prevent unauthorized duplication.

Depending on the policies adopted by each pipeline operator, the basic components and therefore the costs of an access control system can vary. In general, access control systems are based on a ID card-based system with different privileges and permissions (e.g., access cards, ID cards, and contractor cards). The cost of these systems (including hardware and software components) varies from 1000 to 15,000€ for each access depending on the technology that is adopted and whenever the access control installations are digitally interconnected. Integrated electronic access control systems have a higher efficacy in detecting intruders since more complex technologies are used (e.g., digital print recognition). Moreover, access records can be automatically registered and analyzed in real time; doors can be locked and unlocked remotely, on

a predetermined schedule or on demand; and alarms can be generated if unauthorized individuals try to access a facility without permission. Additional functions include security video cameras and the management of the associated video archive. Events associated with door access and with security cameras can be related to each other. For example, a security camera can be set to begin recording when someone enters a particular area, or an alarm can be sent whenever a camera picks up motion during specified hours. The cost of an integrated electronic access system may vary from 10,000 to 50,000€ for each gate, depending on the area to be monitored.

*Patrol:* Traditional patrols can be used by pipeline operators in order to check periodically if anomalies are affecting the pipeline. Ground patrols can be used also as a first response to a warning in order to physically assess the anomalies and conduct an inspection survey. This security measure can be adopted if the pipeline traverses urban areas that are accessible by roads and/or when the length of the pipeline to be controlled is not very long. The cost and the effectiveness of a patrol system depend on a series of factors such as the size and the geographical location of the patrolled pipeline infrastructure, the time needed to reach the control points, the geopolitical risk factors, and the period in which the control should be performed (e.g., day, night, weather conditions). Moreover, the security staff and the characteristics of the patrols fleet (e.g., armed or unarmed vehicles/personnel) may affect the cost-effectiveness of this security measure. In general, agents are highly trained professionals, but in some cases, military personnel with specific security skills may be required. The pipeline surveillance can be organized by each pipeline operator using internal resources and personnel or by outsourcing the security service to specialized companies in order to gain flexibility and reduce costs. These security companies can provide a wide range of patrols and related services depending on the pipeline operator security needs. Specific monitoring software (whose license cost can vary from 700 to 4000€) and secure communication networks can be used to interconnect the patrols among them and with a central security office. Advanced patrol services can include an online reporting system that is able to register (in different formats) all the inspection rounds made by patrols. The cost of the service is affected by several factors, which include duration of the contract, hours to be covered, equipment needed to accomplish the security service, and payment terms. In many cases, the cost of ground patrols is determined on the basis of the number of visits that are accomplished. A reasonable estimation of the price varies from 50 to 1000€/visit. Since most of the pipeline perimeters are simply too long for conventional ground patrols, in order to protect pipeline systems, aerial patrols have become the most suitable solution (Future Fibre Technologies 2013). Aerial patrols provide a bird's-eye view of the pipeline and the surrounding community. The pilots look for anomalies in the ground, suspicious man-made construction, or other suspicious activities that could affect the pipelines. Aerial patrols can be used to flight above the main pipeline along its complete length with regularity depending on the criticality of the pipeline. The effectiveness of aerial patrols is generally higher than the traditional ones since the time needed to reach a control point is drastically lower than traditional ground vehicles. Moreover, pipelines that are located in remote areas and are not served by roads can also be monitored. The higher effectiveness implies an

increased cost (from 5 up to 20 times the cost of a traditional ground patrol) that depends on the type of aerial patrol used (e.g., rotor wing, turbine, piston helicopters), the service provided (e.g., with or without advanced data gathering and data analyzing capabilities), and the skilled personnel required (pilots with special licenses and/or flying experience).

#### **15.4.1.2 Advanced Countermeasures**

*Open-Air Intrusion Detection Sensors:* Perimeter intrusion detection sensors (PIDSs) are based on the core principle of detecting any change above or below a predetermined threshold that indicates that an intrusion event has occurred. For example, an open-air PIDS attached to the fence is able to provide the first warning of an intrusion, detecting the fence climb activity and providing the location of the perimeter violation. This information is then passed to a central control system that activates specific cameras or views, providing visual verification and tracking the intruder inside the pipeline perimeter. There are numerous systems and technologies available to detect intruders. However, each site presents some unique requirements in this regard. When evaluating any PIDS, there are at least three key performance features to be considered:

- the probability of detection (pod);
- the nuisance alarm rate (nar), that consists in the alarms caused by other factors than an intrusion;
- the vulnerability to be defeated or bypassed.

In recent years, in parallel with the development of new materials, there has been a steady move toward developing more sensitive PIDSs, which yield higher POD rates. A number of vendors have introduced fiber-optic sensors that embed a wide range of detection technologies in order to achieve higher detection rates. In fact, they represent reliable and durable sensors being immune to electromagnetic interferences, lightning, radio-frequency transmissions, and magnetic fields. The cost of the fiber-optic sensors generally ranges from 1 to 2€/m of fiber-optic cable. It should be said that the cost depends on the POD and NAR levels. The newer PIDS technologies are also “ranging” or “locating,” which means that instead of simply identifying a zone where an intrusion occurs (which may be several hundred meters long), they give a precise location of the intrusion to a few meters. A deeper layer of defense involves the detection and tracking of an intruder once he has penetrated or breached the perimeter fence. This can be achieved using a variety of technologies. Standard cameras are usually installed, but other modern and innovative technologies (e.g., sensors or radar systems) may also be integrated. Cameras with video motion detection or video analytics are suitable for monitoring, identifying, tracking, and recording intruders: they move away from the fence breach to other areas within the protected site without the operator having to constantly monitor the video or adjust the camera. New generation of long-range cameras, which include electro-optic thermal sensors,

can be used to film in details the surroundings of critical infrastructures offering an instant notification about security violations that occur over large outdoor areas regardless of the weather and light conditions. If cameras are connected to a digital video recorder, they can provide forensic video documentation of an intrusion event. Installation costs of long-range cameras can vary from 20 to 400€/m that needs to be monitored depending on the ground conditions and the technology that is used. The power of the whole surveillance and tracking system is offered by the interconnection of open-air sensors and cameras and by the image processing. Through the image processing, it is possible to detect human intruders with high accuracy while ignoring nuisance alerts such as wind, vibrations, small animals, trees, or blowing trash. An effective surveillance and tracking system requires the integration between sensors and a number of devices (e.g., digital video recorders, network video recorders, closed-circuit television, intercom systems). A single device (e.g., the closed-circuit television) whenever not integrated and incorporated into a complete open-air surveillance and tracking system is less effective from a security point of view.

*Not Open-Air Sensor:* While the traditional open-air sensors, which are able to capture motion and video signals, are suitable for pipelines overground (exposed), sensors based on vibration and acoustic signals need to be used for underground (buried) pipelines especially if located under the water. In order to adequately protect underwater pipelines with the same level of accuracy as for land-based pipelines, subqua sonar systems can be installed at strategic positions along the pipeline. The sonar sensors are able to capture any vibration and acoustic signal in the neighborhood of the pipeline without being affected by nuisance alarms such as the weather or animal activities. Sensors are placed at every meter of a pipeline with a single standard communication optical fiber sensor linked to one or more interrogator units. This security and monitoring solution is capable of detecting and tracking a diver with a close breathing system (combat diver) at up to 700 m and a diver with an open breathing system at up to 1 km. Submersibles and small crafts can also be detected at far greater distances. As soon an anomaly is detected, an alert signal is sent to a central control station where the personnel, using a GPS/GIS system, can locate the attempted sabotage and mitigate the risk in time. Depending on the technology that is used and the depth of the pipeline under the water, installation costs of sonar sensors range from 3 to 10€/m of pipeline segment on which they are installed.

*Remote Sensing Systems:* Sophisticated surveillance systems based on radars or satellites are particularly suitable to monitor pipelines located in critical locations such as inaccessible and unsafe areas. Moreover, remote sensing systems can be used to monitor and map aboveground and underground pipelines in the absence of any type of further ground instrumentation. Movements that happen around the pipeline can be monitored, and real-time pipeline maps can be produced by processing radar satellite images, acquired remotely at regular time intervals by sensibly reducing the need for *in situ* instrumentation and site surveys. In fact, the system can be used to transmit data from remote stations to a central office that, after having analyzed the data, can intervene by adopting the appropriate security actions. Nowadays, newer technologies are available to produce high-resolution images, making the remote sensing system a security measure with attractive cost-effective values for pipeline operators. Three families of remote sensing systems are currently used to monitor

pipelines in real time. The returning data from the sensors can be either analyzed by satellites or aircrafts:

- *LIDAR (airborne and satellite radar)* is used to measure distances by illuminating a target with a laser or an ultraviolet, visible, or near-infrared light and by analyzing the reflected signal at a later stage. This technology is particularly suitable to monitor pipelines located in small areas by using high-resolution images. It is possible to detect movements occurring in the surroundings of the pipelines or changes affecting the area where pipelines are located. Moreover, the LIDAR system can be used even if third elements (e.g., nonmetallic objects, rocks, rain, chemical compounds) are situated between the remote sensor and the target that should be monitored.
- *Scanning Hydrographic Operational Airborne LIDAR Survey (SHOALS)* is used to monitor underwater pipelines. The SHOALS system uses LIDAR technology exploiting the reflective and transmissive properties of the water and of the seafloor. In particular, when a light beam hits the water, part of the energy is reflected off the surface, and the rest is transmitted through the water, unless it is absorbed by particles that are in the water. Using this principle, the SHOALS system gather information about an underwater pipeline by shooting a laser into the water, where a significant amount of energy from the infrared beam is reflected off the surface and detected by receivers.
- *Interferometric synthetic aperture radar (IFSAR)* is used for rapid mapping of wide areas including ground elevations. IFSAR system can simultaneously map planar areas (by mean of X-band) and highlands (by mean of P-band) by operating at relative high altitudes and speeds. X-band and P-band can penetrate clouds, delivering either surface maps of flat areas with or without vegetation or accurate terrain elevations in open areas. These characteristics make IFSAR ideal for mapping large areas of mixed land cover.

The total cost needed to implement a remote sensing system can be relatively high if compared with other security measures. Usually, several private and public investors are grouped in order to finance the realization of a satellite monitoring system. Nowadays, due to the technological evolution, followed by better computers and storage devices, it is possible to realize new generation of smaller and cheaper satellites that are revolutionizing the satellite imagery sector. Several specialized companies, with relatively contained investments of 10–20 million of euro, in the last decades, launched several commercial satellites in order to sell real-time images with high resolution to private companies that are interested in monitoring facilities (e.g., remote pipelines). The price of a satellite image varies from 10 to 15€ per km even if market prices are continuously decreasing as a result of the competition arising from the launch of new satellites. For a detailed report about costs, accuracy, and efficiency in using satellite as a remote sensing system for pipelines, see Palmer (2002).

*Drones:* Open-air surveillance systems can be complemented by drones, which are unmanned aerial vehicles (UAVs) that were initially developed for military purposes. Nowadays, as a result of progress in the high-resolution remote sensing and in

the image processing technology, it is possible to employ small- and medium-sized UAVs and/or unmanned helicopters also for pipeline inspection purposes. Since oil pipelines are usually hundreds or even thousands of kilometers long, sometimes crossing unpopulated areas, their monitoring is a very challenging task for traditional patrols. Therefore, due to their greatest flexibility and versatility, UAVs are very suitable for the monitoring of very long pipeline systems. In particular, UAVs can stay in the air up to 30 h at medium-low altitudes, sending images to a central control station that is responsible for analyzing the gathered data in real time. Several defense contractors are developing UAVs that mount automatic weapons that could be used against possible attackers. The use of UAVs in monitoring petroleum pipelines represents a cost-effective security measure particularly suitable for long-distance pipelines, which may not only eliminate time-consuming and labor-consuming tasks but also raise the efficiency of traditional pipeline patrols. Moreover, due to their capacity to acquire real-time data, pipeline anomalies can be discovered and fixed quickly, thus minimizing the loss in case of attacks. An overall pipeline monitoring system that uses UAVs consists of several ground control stations, unmanned aircrafts, and a commanding software used by ground control stations through which all the unmanned aircrafts can be simultaneously controlled. UAVs can be quite expensive to acquire (in the order of millions of euro), and the costs increase if we consider their functioning and maintenance (in the order of thousands of euro per month). However, UAVs are becoming more affordable with a heavy return on investment. Nowadays, pipeline operators can outsource a surveillance system by means of UAVS instead of buying them. This gives pipeline operators the advantages of the UAVs without the purchase charges and the operating costs. In general, the outsourced surveillance service by using drones is offered by specialized security companies at a fixed price per period, which is in the order of thousands of euro depending of the services offered (e.g., video image recording, simple pipeline monitoring).

#### **15.4.1.3 Recent Technologies**

In recent years, innovative technologies for pipeline surveillance against malicious threats have become more and more available. Nowadays, due to the progress in the field of miniaturized sensors, data processing, and communication system, oil and gas companies have access to robust tools for monitoring of extended and complex pipeline systems. One of the most effective solutions for pipeline monitoring involves a technique known as *distributed acoustic sensing* (DAS), which can convert an optic fiber cable into a listening device. Each section of the cable is used like an acoustic microphone capable of capturing the sound via ground vibrations. The sounds received from the virtual microphones are sent to a processing unit that analyzes them. Subsequently, by using sonar processing techniques, the microphones convert the sounds into a simple graphical display showing what is happening along the cable to the operator.

The DAS system can detect and locate suspicious activities along the entire length of the cable. For example, the seismic sensors can detect the difference between a

mechanical digging and an intruder walking (see Fielding (2012) for more details). The DAS system represents a cost-effective method for monitoring intrusions over long distance. The application of fiber-optic cable as a distributed acoustic sensor has been successfully demonstrated to provide nonintrusive digital pipeline monitoring since it acts as an early warning system, thus allowing operators to act swiftly in the event of an intrusion (Tanimola and Hill 2009).

Alternative cost-effective technologies that have been improved and developed on a large scale from the beginning of twenty-first century can be installed directly on the pipeline surface. In particular, thermal infrared sensors can be used to detect attempts of sabotage. Since the material transported generates frictional heat to the internal wall of the pipe, the pipelines can readily be monitored by using thermal imaging technology. This technique can also be used in regions where the vegetation might obstruct the view of ground patrols or drones.

Other sophisticated ground sensors can be used to monitor remote pipeline networks. In particular, seismic signals of underground vibrations are employed in isolated areas to provide early warning of intruders approaching the protected area. Such systems may be expensive, but by making the remote monitoring of a wider pipeline network possible, pipeline operators can eliminate the need for large numbers of patrols, relying on a few rapid response teams. These sensors are able to protect buried or overground pipelines up to 40 km. They present high values of sensitivity, and at the same time, no nuisance alarms are generated by road crossings and railway lines in close proximity to the pipeline. Seismic sensors can be employed to protect key vulnerability points of a pipeline or to monitor wider areas. Moreover, they can be placed also in geographical locations that present a lack of support infrastructures. In 2003, a high-pressure gas pipeline site in New Jersey, United States, adopted seismic ground sensors, providing the operator sufficient advance notice that an unauthorized vehicles or activity was too close to their pipeline. Further details (strengths, weaknesses, potential causes of nuisance alarms, etc.) concerning modern sensor technologies can be found in Future Fibre Technologies (2013).

Future development of security countermeasures used to protect pipelines will probably follow two directions: cost reduction and increase of efficacy as a consequence of the growth of the detection rate or/and the reduction of the nuisance alarms. Cost reduction can go hand in hand with the increase of the efficacy thanks to the development of new materials and technologies with higher sensitivity rates. It should be highlighted that in many sensors the increase in sensitivity does not result in a better efficacy due to the growing number of nuisance alarms (an alarm is reported without any real intrusion). Therefore, nowadays, a significant amount of technology development is focused on processing external signals in order to reduce the number of nuisance alarms that are typically generated by environmental conditions such as wind, rain, passing traffic, and lightning. Before the advent of the modern programming languages and the increase of the computers' computational power, the existing techniques employed to control nuisance alarms were based on the temporary reduction of the sensitivity capability within short time intervals characterized by a high level of environmental noise (Future Fibre Technologies 2013). Unfortunately, the reduced sensitivity to intrusions implied a reduced

probability of detection, especially during adverse weather conditions. In order to overcome this problem, modern sensors use advanced multiparameter signal processing techniques such as artificial intelligence (AI), artificial neural networks (i.e., models inspired by an animal brain aimed at machine learning and pattern recognition), and data mining. In fact, these techniques are used to analyze external data by distinguishing between intruders and environmental disturbances, thus increasing the accuracy and the performance of the security sensors.

To conclude, further development of the security measures based on radar systems will be achieved thanks to the improved capability to memorize and generate high-resolution images together with the development of faster and robust protocols for satellite communication. In the short run, the need for safer and cheaper operations will also lead to the exploitation of drones with a higher autonomy to conduct geo-physical survey missions and using various types of sensors aimed at preventing terroristic attacks.

#### **15.4.2 Integration of Security Layers**

The aforementioned perimeter protection measures can be integrated into a global surveillance system. In general, this approach is known as the *onionskin principle*, which has been developed to protect critical infrastructure by combining several security elements, technologies, and strategies into an integral security system. In particular, a security information management (SIM) system needs to be adopted in order to interconnect multiple existing security systems into a single interface that automates the notifications and interactions between security components (e.g., detectors in the field, sensors mounted on the fence, cameras, and radar).

All of the gathered signals are then analyzed to instantly identify possible malicious threats that require urgent attention. With the advent of mobile devices, it is possible to relay detailed information about possible intrusions in real time to mobile security forces in the field. The aim of an SIM system is therefore to provide the warning that an intruder has breached the pipeline perimeter, to visually verify the intrusion, to track the intruder once he is inside the perimeter, and to select the appropriate security responses before he/she reaches the target. Moreover, a SIM system can provide a total picture of a security accident in order to enable the responders to have a complete situational awareness and respond to it in the most effective manner.

#### **15.4.3 Protection from Cyberattacks**

The control systems used by pipeline operators to manage their infrastructure are of capital importance to guarantee the pipelines' safety and efficiency. The growing convergence of information technology and control systems goes hand in hand with an increased exposure of the pipeline infrastructure to cyberattacks. Developing and implementing appropriate cybersecurity countermeasures can reduce both the risk to be attacked and the negative consequences of a cyberattack.

Possible cyber threats may affect the following components of a pipeline infrastructure: interconnected hardware and software, computers, databases, and control and monitoring devices. In order to implement an effective cybersecurity strategy, each pipeline operator should adopt appropriate methodologies, standards, and best practices. Before the implementation of a risk management plan, the cyber assets should be evaluated and classified using the following criteria:

- Critical cyber assets that are essential to safety and/or reliability of the pipeline. Enhanced security measures should be applied to these assets;
- Noncritical cyber assets that are not essential to safety and/or reliability of the pipeline.

The following measures, adapted from the Transport Security Administration (2011), can be implemented to protect the cyber critical assets:

- *Basic cybersecurity measures* that can be applied to all cyber assets includes:
  - policies and procedures both for monitoring and detecting cyber intrusions and for handling and reporting cyber accidents;
  - training of the personnel to increase the cybersecurity awareness;
  - firewalls and other protections aimed at segregating and protecting the control systems from the business network and the internet network;
  - access control policies for local and remote users, guests, and customers;
- *Enhanced cybersecurity measures* that can be applied to all critical cyber assets comprises:
  - access restriction to control systems through the use of an appropriate combination of locked facilities, passwords, communication gateways, access control lists, authenticators, and separation of duties;
  - risk assessment before the implementation of wireless networks;
  - periodic vulnerability assessments of the control system and of the cybersecurity measures.

## 15.5 SECURITY RISK ASSESSMENT AND COUNTERMEASURES SELECTION

In general, risk assessment is an analytical process through which an operator determines the types of adverse events or conditions that might impact negatively on the pipeline. Risk assessment also determines the (qualitative, semiquantitative, or quantitative) likelihood of those episodes or conditions that may lead to a loss of integrity and the nature and severity of the consequences that might occur due to a failure.

The ultimate goal of risk assessment is to identify the most significant risks so that an operator can develop an effective and prioritized prevention/detection/mitigation

plan to address the risks. The more information is available, the more accurate the risk assessment process. In general, risk assessment involves several activities:

- gathering and integration of existing data;
- threats and security risk analysis;
- security risk determination;
- security risk prioritization;
- countermeasures selection.

After the technical risk assessment activities, risk management needs to take decisions based both on the available information with respect to security risks and based on the available budgets. This is a more company policy-related activity. The security risk and the emergency plan worked out by security risk management are functions of threats, vulnerabilities, and consequences and all countermeasures taken to treat the security risk. The most effective security programs employ a risk management process that facilitates proactive planning and decision making to mitigate risks for pipeline assets. General steps include:

- criticality assessments (determine facility criticality);
- threat assessments (identify known or potential adversaries);
- vulnerability assessments (identify security weaknesses);
- risk assessments (based on threat, vulnerability, and criticality assessment findings);
- risk mitigation (determine and implement appropriate risk reduction countermeasures);
- ongoing risk management (monitor, reassess, and modify the program);
- emergency plan (evacuation, pipeline recovery, etc.).

There are multiple risk assessment methodologies, and each operator should determine the most appropriate process and methodology for the implementation of their corporate security plan and the facilities comprising their pipeline system. In the case of a pipeline network, the security risk assessment procedure elaborated and explained by Reniers and Dullaert (2012) may be used. At the end of this pipeline security risk assessment exercise, the user disposes of (relative) *pipeline segment risk* data as well as (relative) *pipeline route risk* data. Assuming that the security risk analyst determines a set of available countermeasures and defense strategies for the different pipeline segments and/or for the pipeline routes, a selection of the most effective countermeasures with respect to the available budget (either for a single pipeline segment or for a pipeline route) can be calculated and determined (the costs of the countermeasures need to be known in advance). The mathematical approach that can be used to solve these problems of optimal allocation of security resources is the knapsack problem. Reniers et al. (2013) explain how this well-known technique from operations research is easy to use in case of security optimization problems.

The goal is to determine the optimal bundle of security countermeasures to protect a pipeline infrastructure given a limited security budget. The model can be applied either to a single pipeline segment or to a whole pipeline route. The knapsack problem used for the security optimization problem implies the minimization of the total risk (or symmetrically the maximization of total benefit offered by the selected security countermeasures) while respecting a cost constraint. As a matter of fact, the total cost of the selected countermeasures cannot be larger than the available budget for security. As also mentioned by Reniers et al. (2013), some assumptions are implicitly taken in the knapsack problem for the selection of security countermeasures:

1. a countermeasure is either taken or not (it cannot be partially taken);
2. the total benefit (negative risk) of all countermeasures is the sum of the individual benefits of the chosen countermeasures;
3. the total cost of all countermeasures is the sum of the costs of the individual countermeasures;
4. the countermeasures can be independently implemented without consequences for the other countermeasures. to refine the knapsack problems, because some of the assumptions are not always realistic, additional constraints can be inserted into the mathematical formulations, and the problems can be adapted to specific circumstances/situations of each pipeline operator.

### 15.5.1 Illustrative Example

It is possible to apply the knapsack model for the selection of security countermeasures to solve a strategic problem that many oil pipeline operators encounter on a regular basis, whenever they have to define the best security measures to protect a pipeline network from possible malicious threats. The pipeline network that needs to be secured connects a refinery to a storage area located in a desert area. The length of the whole overground pipeline network is 500 km. The available budget to secure the entire pipeline route is 4 million of US dollars. Given the characteristics of the pipeline network, at the end of the risk assessment phase, the risk analyst has short-listed a set containing a restricted number of security countermeasures. A short description of the perimeter protection measures together with their total cost (including maintenance costs) in the evaluation period (e.g., 5 years), their theoretic efficacy, and their risk reduction (both determined by security managers) is shown in Table 15.2. In particular, the risk reduction can be seen as the benefit, offered by a countermeasure, in reducing the risk faced by the pipeline network.

Using the approach of Reniers and Dullaert (2012), the optimal set of security measure can be defined assuring the highest level of threat detection without exceeding the security budget. For this specific scenario, the optimal solution implements countermeasures B, G, and H for a total budget of \$3.45mio and a total risk reduction of 1730 units.

**TABLE 15.2 Available Countermeasures**

Countermeasures		Efficacy (%)	Risk Reduction	Cost in \$ (x1.000)
Id		Description		
A	Fences with active and passive infrared remote sensors	85.7	600	3200
B	Three unarmed UAVs	87.4	550	1200
C	Three armed UAVs	89.2	470	1800
D	Two helicopters equipped with three armed guards	83.4	700	2500
E	LIDAR radar system	90.3	400	1450
F	Fences with cameras	81.7	780	2900
G	Buried fiber-optic intruder sensors	89.2	530	1400
H	Thermal infrared remote sensors	83.5	650	850

## 15.6 CONCLUSIONS

In this chapter, we investigated different aspects related to pipeline security. After a brief description and classification of the deliberate accidents that may be inflicted on pipelines, the most important information and data that need to be appropriately managed by pipeline operators were presented. Through an adequate information management, pipeline operators can prevent intentional attacks and limit their consequences by adopting appropriate security countermeasures.

Subsequently, a general survey of available methods that can be adopted by pipeline operators to contrast attacks or other criminal activities was carried out. Particular attention was given to perimeter security systems, which are commonly used to defend the boundaries of critical infrastructure, deter any malicious acts, detect such acts, implement measures to delay attacks, and help security agents or the police to detain any intruders. The key element to secure pipelines is the use of a multilayered approach. The more layers an intruder needs to get through to reach his target, the more likely he will be detected and therefore the more secure the pipeline. Each security layer can have different properties (e.g., system durability, maximum detection capability, ability to quickly and accurately pinpoint the location of intrusion, installation cost and maintenance), advantages, and disadvantages.

In order to choose the more suitable countermeasure, the risk profile and the possible threats for the pipeline should be investigated. These concepts rely on the characteristics of the pipeline and on the location in which the infrastructure is built. The presence of accurate information is therefore crucial.

Once all risk factors have been identified and measured, using an appropriate risk assessment methodology, the expectations of the pipeline operator and the available intruder response mechanisms should be taken into account. Having in mind the operator's budget, it is possible to identify the best effective

countermeasure (or a combination of them) to protect a pipeline site against deliberate and planned attacks via a decision support system. In this chapter, we presented a simple model based on the knapsack problem that can be used to support such decisions.

## REFERENCES

- Boston.com. (2010, July 21). Oil spill in Dalian, China. Retrieved August 9, 2013 from [http://www.boston.com/bigpicture/2010/07/oil\\_spill\\_in\\_dalian\\_china.html](http://www.boston.com/bigpicture/2010/07/oil_spill_in_dalian_china.html) (accessed March 3, 2015).
- Baker, M. and Fessler, R. R. (2008). *Pipeline Corrosion: Final Report*. Washington, DC: U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration Office of Pipeline Safety.
- Baran, Z. (2007). EU Energy Security: Time to End Russian Leverage. *The Washington Quarterly*, 30 (4), 131–144.
- Chow, E., Hendrix, L. E., Herberg, M. E., Itoh, S., Kong, B., Lall, M., et al. (2010). *Pipeline Politics in Asia: The Intersection of Demand, Energy Markets, and Supply Routes*. Seattle, WA: The National Bureau of Asian Research.
- Clayton, M. (2013). *Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage*. Boston, MA: Christian Science Monitor.
- Cohen, A. (2006). The North European Gas Pipeline Threatens Europe's Energy Security. Backgrounder, The Heritage Foundation No. 1980, Washington DC, October 26, pp. 2–11. Retrieved from <http://www.massenbach-world.de/media/116800689f529cf2ffff831aac144225.pdf> (accessed March 3, 2015).
- Department of Homeland Security. (2003). *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*. Washington, DC: The White House.
- European Commission. (2011). *Assessing the Case for EU Legislation on the Safety and the Possible Impacts of Such an Initiative*. Brussels: Directorate General Environment, European Commission.
- European Gas Pipeline Incident Data Group. (2011). *Gas Pipeline Incidents*. Groningen: European Gas Pipeline Incident Data Group.
- Farah, D. (2012). Terrorist-Criminal Pipelines and Criminalized States. *PRISM*, 2 (3), 15–32.
- Fielding, A. (2012). Pipeline Security: New Technology For Today's Demanding Environment. *Pipeline & Gas Journal*, 239 (5): 1–5.
- Future Fibre Technologies. (2013). *The Boundary of Security 2013: Global Trends in Perimeter Security*. Mulgrave: Future Fibre Technologies Pty Ltd.
- Gasol PLC. (2012). *African gas for the Next Generation*. Annual report and accounts. London: Gasol PLC.
- Hernandez, M. (2007). *Mexican Rebels Claim Pipeline Attacks*. Washington, DC: Associated Press.
- Institute for the Analysis of Global Security. (2008). *Iraq Pipeline Watch*. Retrieved October 15, 2013 from <http://www.iags.org/iraqpipelinetwatch.htm> (accessed March 3, 2015).
- Institute for the Analysis of Global Security. (2013). *Oil, Terrorism and Drugs Intermingle in Colombia. Energy Security Brief*. Potomac, MD: Institute for the Analysis of Global Security.

- Johnston, P. (2008). *Oil and Terrorism: Al Qaeda's Threat*. Ottawa: Defence R&D Canada, Centre for Operational Research & Analysis.
- Khan, A. (2006 February 20). Six More Bombings Rock Loti and Pirkoh. *Daily Times*.
- Kuik, G. and Bolt, R. (2003). Safety in European Gas Transmission Pipelines; EGIG Shows its Continuing Improving Safety Performance. *22nd IGU World Gas Conference*. Tokyo, Japan, June 1–5, 2003.
- Kupchinsky, R. (2005). *Chechnya: Stolen Oil and Purchased Guns*. Retrieved November 3, 2013 from <http://www.rferl.org/articleprintview/1062391.html> (accessed March 3, 2015).
- Lennon, M. (2013, July 1). Cyber Attacks Targeted Key Components of Natural Gas Pipeline Systems. *Security Week*.
- Luft, G. (2005). Pipeline Sabotage is terrorist's Weapon of Choice. *Pipeline & Gas Journal*, 232 (2), 42.
- Makarenko, T. (2003). *The Crime Terror Nexus*. London: C. Hurst & Co. Publisher Ltd.
- Matheson, M. and Cooper, B. S. (2004). Security Planning and Preparedness in the Oil Pipeline Industry. In *The Oil & Gas Review*. London: Touch Briefings, pp. 104–108.
- McDermott, M. (2004). Terror on the Home Front. *Security*, 12–17.
- Moteff, J. and Parfomak, P. (2004). Critical Infrastructure and Key Assets: Definition and Identification. *Congressional Research Service Report for Congress*. Washington, DC.
- Muhlbauer, W. K. (2004). *Pipeline Risk Management Manual: Ideas, Techniques, and Resources*. Amsterdam: Elsevier/Gulf Professional Publishing.
- National Pipeline Mapping System. (2012). *Operator Standards Manual*. Washington, DC: U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration.
- Office of Cybersecurity and Communications. (2009). *CYBER STORM II*. Washington, DC: U.S. Department of Homeland Security, National Cyber Security Division.
- Onuoha, F. (2007). Poverty, Pipeline Vandalisation/Explosion and Human Security. *African Security Review*, 16 (2), 94–108.
- Owen, A. (2013). *Calculating the Quality of Performance of a Perimeter Intrusion Detection System*. White Papers. Hartnett Close Mulgrave: Future Fibre Technologies Pty Ltd, 107–108.
- Palmer, A. (2002). *Appraisal of Pipeline Surveillance by High Resolution Satellite*. Newcastle upon Tyne: HSE Books.
- Parfomak, P. W. (2012). Keeping America's Pipelines Safe and Secure: Key Issues for Congress. *CRS Report for Congress*. Washington, DC.
- Rapier, R. (2010). *Oil Infrastructure and Terrorism*. Energy Trends Report. Sheffield: Energy Trends Insider.
- ReniersG. and Dullaert, W. (2012). TePiTri: A Screening Method for Assessing Terrorist-Related Pipeline Transport Risks. *Security Journal*, 25 (2), 173–186.
- Reniers, G., Sørensen, K., and Dullaert, W. (2013). A Multi-Attribute Systemic Risk Index for Comparing and Prioritizing Chemical Industrial Areas. *Reliability Engineering & System Safety*, 98 (1), 35–42.
- Reuters. (2013, July 29). Retrieved August 9, 2013 from <http://www.reuters.com/article/2013/07/30/colombia-oil-explosion-idUSL1N0FZ1SL20130730> (accessed March 3, 2015).
- Shreeve, J. (2006). Science & Technology: The Enemy Within. *Scientific American*, p. 8.

- Simonoff, J. S., Restrepo, C. E., and Zimmerman, R. (2005). *Trends for Oil and Gas Terrorist Attacks*. Research Report No. 2. Hanover, NH: Institute for Information Infrastructure Protection, Dartmouth College.
- Steinhäusler, F., Furthner, P., Heidegger, W., Rydell, S., and Zaitseva, L. (2008). Security Risks to the Oil and Gas Industry: Terrorist Capabilities. *Strategic Insights*, VII (1): 1–44.
- Steinhäusler, F., Furthner, P., De la Cruz, A., Palade, B., and Soares, P. (2009). Applying Advanced Technology for Threat Assessment: A Case Study of the BTC Pipeline. *Journal of Energy Security*, (6): 1–10.
- Subramanian, N. (2008). Improving Security of Oil Pipeline SCADA Systems Using Service-Oriented Architectures. In *On the Move to Meaningful Internet Systems: OTM Workshops* (pp. 344–353). R. Meersman, Z. Tari, and P. Herrero (Eds.). Berlin/Heidelberg: Springer.
- Tanimola, F. and Hill, D. (2009). Distributed Fibre Optic Sensors for Pipeline Protection. *Journal of Natural Gas Science and Engineering*, 1, 4–5, 134–143.
- Taylor, D. (2012). *Oil Pipeline, Platform And Refinery False-Flag Terror Attacks Imminent*. Retrieved from <http://Truther.org> (accessed March 3, 2015).
- Telhami, S. (2002). The Persian Gulf: Understanding the American Oil Strategy. *The Brookings Review*, 20 (2), 32–35.
- The American Society of Mechanical Engineers. (2004). *Managing System Integrity of Gas Pipelines*. New York: The American Society of Mechanical Engineers.
- The White House. (2000). *Defending America's Cyberspace: National Plan for Information Systems Protection. Version 1.0*. An Invitation to a Dialogue. Washington, DC: The White House.
- Transport Security Administration. (2011). *Pipeline Security Guidelines*. Washington, DC: U.S. Department of Homeland Security.
- Transportation Sector Network Management. (2006). *Pipeline Security Smart Practices*. Washington, DC: U.S. Department of Homeland Security Transportation Security Administration.
- U.S. Department of Homeland Security. (2005). *Potential Indicators of Terrorist Activity. Infrastructure Category: Petroleum Pipelines*. Washington, DC: U.S. Department of Homeland Security.
- U.S. Department of Homeland Security. (2008). *Fact Sheet: Executive Order on Cybersecurity. Presidential Policy Directive on Critical Infrastructure Security and Resilience*. Washington, DC: U.S. Department of Homeland Security.
- U.S. Department of Transportation. (2013). *Pipeline and Hazardous Materials Safety Administration, Pipeline Incidents and Mileage Reports*. Washington, DC: Office of Pipeline Safety. Retrieved from <http://ops.dot.gov/stats/stats.htm> (accessed on March 3, 2015).
- U.S. Office of Homeland Security. (2002). *The National Strategy for Homeland Security*. Washington, DC: U.S. Department of Homeland Security.
- Ya'ar, C. (2013). Egypt's Gas Pipeline Comes Under Attack. *Arutz Sheva*, July 7, 2013.



## **SECTION III**

---

### **THE ROLE OF TRANSPORTATION IN EVACUATION**



---

# 16

---

## EVACUATION FROM DISASTER ZONES: LESSONS FROM RECENT DISASTERS IN AUSTRALIA AND JAPAN

DANIEL BALDWIN HESS<sup>1</sup> AND CHRISTINA M. FARRELL<sup>2</sup>

<sup>1</sup>*Department of Urban and Regional Planning, University at Buffalo,  
State University of New York, Buffalo, NY, USA*

<sup>2</sup>*Regional Institute, University at Buffalo, State University of New York,  
Buffalo, NY, USA*

### 16.1 INTRODUCTION

Preparing for disasters that require large-scale evacuation is an enormous challenge for disaster planners and emergency managers. Various postdisaster assessments conclude that many local emergency planning processes devote insufficient attention to the challenges of large-scale evacuation (Hess & Gotham 2007). According to a 2007 Rand Institute study of governmental response to Hurricane Katrina, one of the greatest obstacles to the provision of relief was the inadequacy of transportation assets and personnel (Rand Corporation 2007). Considering various types of disasters that may befall human settlements—including natural disaster, technological (or man-made) disasters, and malevolent acts (Dotson & Jones 2005)—most state and local municipalities remain ill prepared to handle large-scale evacuations from urban areas. A key problem learned from past disasters is a lack of coordination for local and regional emergency transportation for the responding medical assistance

volunteers and especially the movement or evacuation of patients and special needs populations (Tierney et al. 2001; Sternberg & Lee 2009).

Recent disasters in North America—both notice events and no-notice events—underscore an urgent need for improved evacuation capability. In April 2013, an explosion at a fertilizer plant in West Texas resulted in injury, property, damage, and death (Fernandez & Schwartz 2013). Emergency workers were at the scene fighting a fire that preceded the explosion, which required the immediate evacuation—aided by spontaneous volunteers—of a nearby nursing home (Santos & Krauss 2013). In October 2012, Hurricane Sandy, after its start in the Caribbean Sea, struck the mid-Atlantic US state and New England, eventually killing more than 250 people in seven countries (Saul 2012). The “superstorm” formed from a confluence of extreme weather conditions and included record extreme pressure and a record tidal surge, producing snow in the West Virginia mountains. The hurricane produced coastal devastation and tens of thousands of downed trees. Humans were impacted through unprecedented disruptions to power, transportation, and communication networks. Coastal areas were particularly vulnerable to storm surges, and in New York City, improved evacuation planning efforts during the previous decade among public agencies helped to move many people to safety by closing public transportation systems before the storm (Kaufman et al. 2012) and enacting a zone-based evacuation plan three days before the storm, first tested one year earlier when Hurricane Irene struck the New York City metropolitan region (Hess et al. 2013b).

Choosing whether or not to order a mandatory evacuation is a complex and critical decision that emergency managers and government leaders often face when the most severe disasters strike. Forming a judgment about the need to evacuate becomes more challenging when emergency managers consider the sacrifice individuals, families, and communities must endure during the execution of an evacuation (Fairchild et al. 2006). Therefore, in making this decision, the risk of injuries or deaths stemming from a disaster must be judged to be at a level that exceeds the costs of evacuating; that is to say that, with a high degree of certainty, the outcomes of undertaking an evacuation are surpassed by its costs (in terms of property damage, injury, and loss of life) (Fairchild et al. 2006). This rule frames the decision to evacuate, a decision that occurs at two levels: (i) governmental decisions and (ii) the individual actions.

Local government leaders are best positioned to protect citizens and prevent localities from being overwhelmed by the effects of a disaster (Somers & Svara 2009). Thus, local emergency managers play a critical role in deciding if evacuation is necessary and what resources, if any, are to be requested from higher levels of government to conduct an evacuation. While guiding principles regarding the decision to issue an evacuation order are likely identified in written emergency plans, the clarity and effectiveness of these principles vary from one municipality to the next and from one emergency situation to the next. Furthermore, municipal officials will undoubtedly base their judgment on certain factors to varying degrees based on the content and reliability of the information they receive, personal perception of emergency incidents, and even intuition.

Shelter in place has become a preferred disaster response strategy in many disaster plans and emergency response policies in the United States, because people’s safety

is jeopardized when they travel to evacuate. Only in the most severe disaster situations do certain planning processes include large-scale evacuation as an option. We have argued in previous research (Hess & Arendt 2006; Hess & Gotham 2007; Hess & Arendt 2009; Hess et al. 2013a; Hess et al. 2013b), however, that it is critically important for cities, metropolitan areas, and regions to be prepared for the possibility—however unlikely—of a large-scale evacuation in which everyone must move to a safe zone to avoid exposure to the effects of disaster and potential injury or loss of life.

To enhance scholarly knowledge of large-scale evacuation precipitated by high-impact disasters, we evaluate recent high-profile disasters that included evacuation from danger zones. Using recent disasters in Australia and Japan, we describe evacuation plans and outcomes of disasters, and we explore evacuation readiness, implementation, and outcomes with a full understanding of disasters and their consequences. In this chapter, we explore factors that influence the decision to evacuate from two aspects: (i) governmental decisions and (ii) the individual actions. This work thus builds upon research in evacuation policy and planning (Hess et al. 2013a; Hess et al. 2013b), multimodal evacuation (Hess 2006; Hess & Gotham 2007), disaster response in the United States (Hess & Arendt 2006; Hess & Arendt 2009), and evacuation for vulnerable groups (Hess 2007) and research about people who cannot self-evacuate (Renne 2006; Hess & Gotham 2007; Renne et al. 2008; Renne et al. 2009; Hess et al. 2013a). We intentionally choose a no-notice event (an earthquake, with linked resultant disasters) and a limited notice event (wildfires) since these types of events critically test emergency preparedness and response. Since much of the focus of research in recent years has been on disasters in urban settings, we intentionally choose locations with lower population density and population distributed throughout a network of small towns.

To fully assess disasters and their outcomes, we review published research and government reports from the two disasters and synthesize these with published research about disasters and evacuation. This knowledge helps frame an understanding of emergency incidents that define the milieu of events that surround decision making about evacuation. We review the outcomes of emergency planning and practice vis-à-vis evacuation, and we synthesize findings from scholarly literature with two case studies to provide recommendations about disaster readiness.

## 16.2 EMERGENCY EVACUATION: PLANNING AND PRACTICE

Local governments generally possess primary responsibility for emergency management operations (in the United States as well as in most other countries) and play a crucial role during evacuations and in emergency management in general (Henstra 2010). Chief executive officers of municipalities and counties (such as a mayor) and chief executive officers of a state (such as a governor) have the authority to declare a state of disaster (even in anticipation of a predicted event that has not yet begun) and order a mandatory evacuation. State governments, especially governors' offices, are typically afforded comparable authority to issue an evacuation order

(Fairchild et al. 2006). The federal government can act as coordinator and partner, assisting local and state governments when capacity to respond is exceeded by the effects of an incident (McGuire & Schneck 2010).<sup>1</sup>

In an evacuation ordered by government leaders, all individuals are required by law to evacuate according to local, county, or state ordinance. (A US House of Representatives (2006) report found that failing to comply with a mandatory evacuation order is illegal, applying the reasoning that this behavior would inevitably put responders' lives at risk.) Evacuation may be policed by law enforcement. A person's willingness or ability to vacate an area with necessary urgency can be limited, as demonstrated during Hurricane Katrina, when some individuals chose not to evacuate and later found evacuation impossible (due to floods) and required rescue by emergency personnel (Lindell et al. 2005; Elder et al. 2007). Even when people are adequately informed about disaster risks, it cannot be assumed (i) that an official warning will provide individuals with a sound appreciation of the implications of that warning and (ii) that this awareness, if realized, leads people to take recommended precautionary actions (Sims & Baumann 1983). It can therefore be reasoned that, in general, during emergency incidents, individuals will pursue the action that they deem to be most sensible based on the information they are provided and their own perspective (Sorensen et al. 2004).

The most fundamental predictor of evacuation participation is an individual's knowledge about an evacuation order (Baker 1991; Hasan et al. 2011). Moreover, the reliability of the order, its source, and any information corroborating that order as a formative condition of an individual's evacuation choice cannot be understated (Sorensen 1991; Elder et al. 2007; Hasan et al. 2011). Even when an official command is placed, it is estimated that one-third of the public will not necessarily follow evacuation orders (Carter 1979).

Greater clarity of evacuation procedures and credibility of information sources (e.g., known government official) is associated with higher compliance with evacuation orders (Sims & Baumann 1983). Also, the risk level of a specific location, along with residents' perception of this risk, both play a part in the likelihood of evacuating (Baker 1991). Television and the saturation of news and weather media prompt increasing levels of evacuation participation through disaster reports and footage, which can sometimes be sensational (Sims & Baumann 1983; Elder et al. 2007). However, during many emergency events, an evacuation order may become muddled (especially with increased use of social media) and evacuation orders may not be heeded (Sims & Baumann 1983; Baker 1991; Sorensen et al. 2004).

<sup>1</sup>This structure was initially put into place in the United States by the Disaster Relief Act Amendments of 1974, frequently referred to as the Stafford Act (McCarthy 2011). This act bestowed national government with power to aid in disaster relief on the conditions that (i) a governor requests such assistance, (ii) the degree of necessary response does indeed surpass state capacity, and (iii) a governor must put into effect the state's emergency plan (Fairchild et al. 2006). Additionally, federal courts also maintain the authority to order evacuations during severe emergencies (Thames Shipyard and Repair Co. v. United States 2003).

When a large-scale evacuation is not warranted, emergency managers may elect to “keep and provide” for affected populations in a disaster zone, a strategy known as “shelter in place,” which is thought under certain conditions to be more reasonable and safer than evacuating (Cutter & Smith 2009). Evacuation may be a more favorable option for incidents in which people have ample time to evacuate before a disaster occurs (e.g., before a toxic plume arrives). Shelter in place has indeed proven to be a wiser option than large-scale evacuation under certain circumstances (Mannan & Kilpatrick 2000).

During a disaster, people will choose the action that they judge to be the best for their safety and well-being (Sorensen et al. 2004). For optimal implementation of an emergency evacuation, institutional partnerships between government, residents, and other actors are essential, as is a high degree of disaster preparedness and education at the community and government levels (Glotzer et al. 2007). Factors found to influence whether or not an evacuation should, or will, occur in the event of an emergency include (Hess et al. 2013a; Hess et al. 2013b):

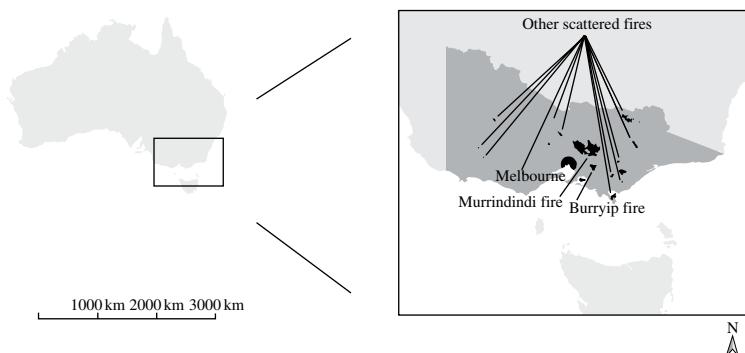
- Presence and timing of disaster warning period (i.e., a “notice” event or “no-notice” event”)
- Severity, nature, and duration of disaster effects (including weather and climate conditions)
- Resources available for sheltering
- Condition of critical infrastructure
- Community context (preparedness/training of individuals, demographic composition of community)
- Policy context (preparedness/training of local government)

In practice, however, a decision to actually undertake an evacuation, either by a municipality or by an individual, may not be entirely reliant on a concrete set of identifiable factors. This is especially true when considering the possibility of a “double event,” e.g., a nuclear spill in the aftermath of an earthquake. Whether or not to mandate an evacuation therefore arises as a “wicked problem” (Rittel & Webber 1973) in that it most often cannot be determined by a replicable, systematic formula.

### 16.3 CASE 1: RISING HEAT IN AUSTRALIA (2009)

#### 16.3.1 Disaster Overview: Rising Heat

Bushfires that swept across Australia’s southern state of Victoria in February 2009 rank second among Australia’s worst natural disasters and, in terms of fatalities, among the top ten wildfires/bushfires in the world (Cameron et al. 2009). In late January 2009, Victoria suffered one of its most severe and prolonged heat waves, which peaked on February 7, 2009 (“Black Saturday”), when Victoria endured numerous record-breaking temperatures. Melbourne, the capital, reached 46.4°C (116°F)—its hottest day on record (Teague et al. 2010).



**FIGURE 16.1** Map of 2009 bushfire sites in Australia.

Several disaster events comprise Black Saturday, including numerous wildfires (see Fig. 16.1) that started naturally and by human activity. Nine of fifteen fires were caused by direct or indirect result of human activity—five were associated with electrical failure, and four were deemed suspicious (Teague et al. 2010). Weather, however, was responsible for the intensity of the fires. In the days leading up to February 7, four key meteorological elements affecting the spread of fire—air temperature, relative humidity, wind speed and direction, and atmospheric stability—were at their most extreme (Teague et al. 2010), prompting Victoria's premier to warn citizens to be vigilant in these extreme conditions (Teague et al. 2010).

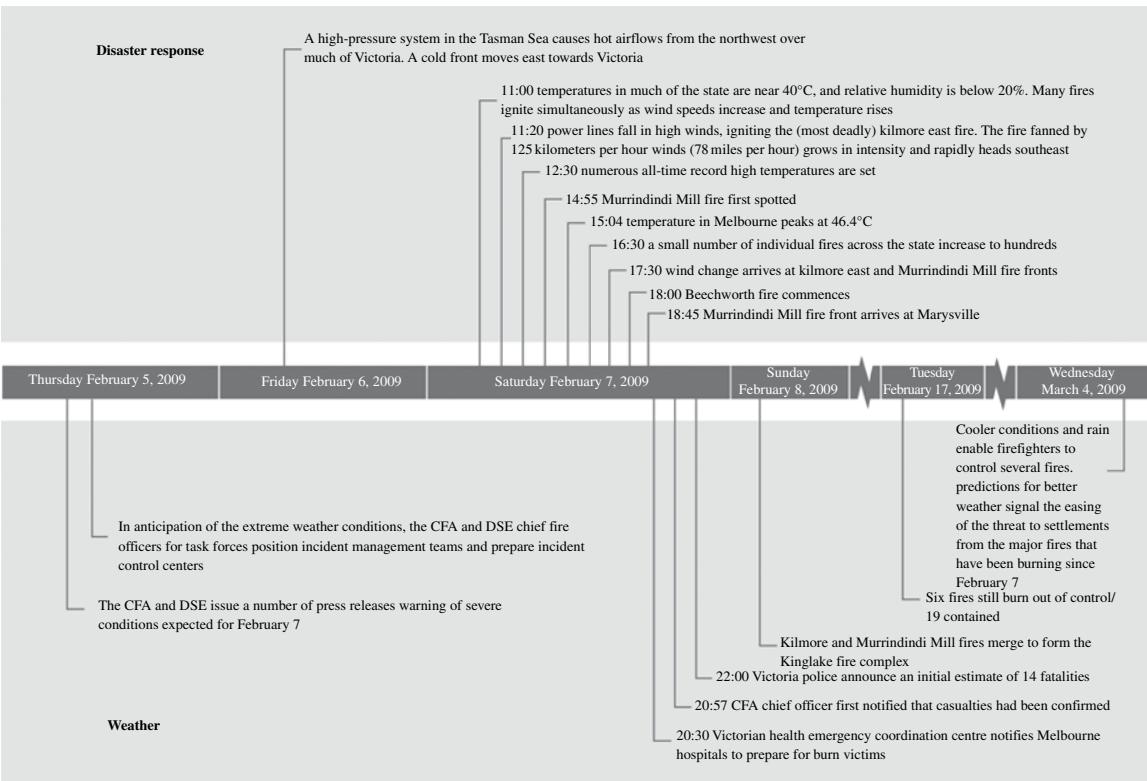
Although the wildfires varied in their size and impacts, the most severe of the fires shared the following characteristics: crews could not contain the rapid fire spread; crews could not control fires in forested areas; powerful convection columns were generated above the fires; extensive forward spotting occurred as a result of the characteristics of the “fuel” (a term used to describe anything that combusts, generally vegetation) for wildfires and winds gusting up to 100 kilometers per hour (62 miles per hour); and late in the day, a wind change altered the direction of fire spread and extended the fire-front (Teague et al. 2010) (see Fig. 16.2). On Black Saturday, a 100-point scale<sup>2</sup> used to rate the severity of fires was exceeded across the state, with ratings of 120 to 190 points (O’Neill & Handmer 2012). It was not until mid-March 2009 that favorable conditions aided containment efforts and most of the fires were extinguished.

This was the first time that such widespread and intense bushfires had occurred in an urban–rural interface, and the resulting loss of human lives (173) and burned landscape (430,000ha or 1.1 million acres) were unprecedented (Paveglio et al. 2012).

### 16.3.2 Emergency Preparedness and Response

**16.3.2.1 Stay or Go Policy** Emergency management and elected officials made decisions in the context of Black Saturday that were motivated by an overarching policy for community safety in bushfires. That policy, “Prepare, Stay and Defend, or

<sup>2</sup>The Forest Fire Danger Index can be used to better understand this perfect storm of weather conditions. FFDI, designed on a 0 to 100 scale, includes a number of meteorological variables. FFDI ratings of 50 and above describe an “extreme” fire where suppression is difficult (O’Neill & Handmer 2012).



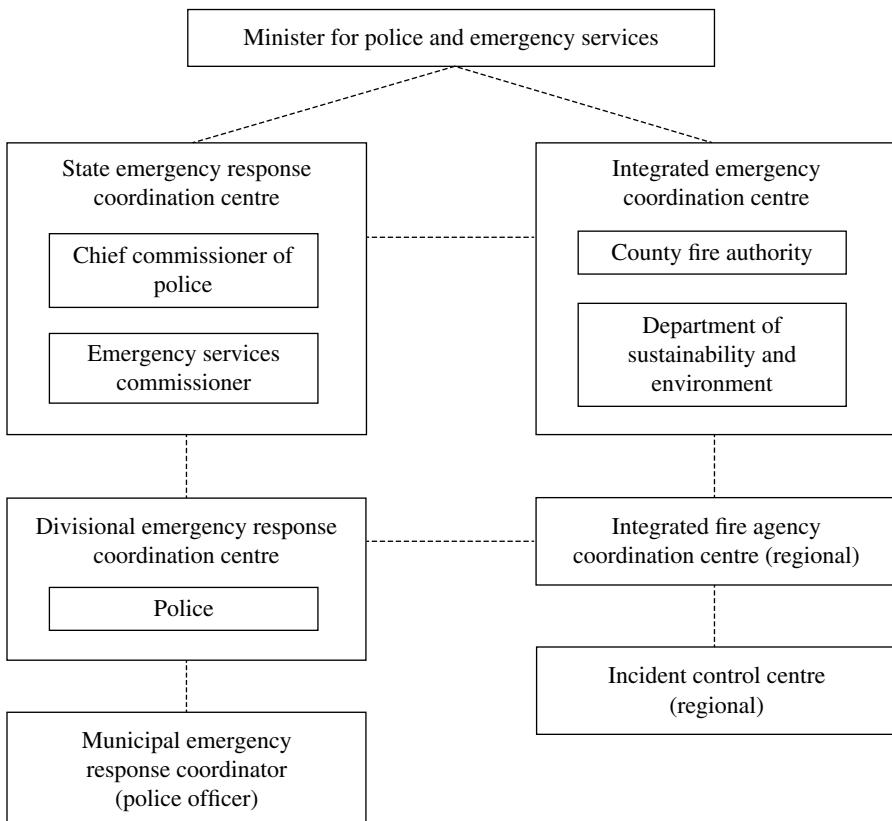
**FIGURE 16.2** Timeline of events in Australia. Adapted from (<http://blacksaturdayfires.wikispaces.com/Timelines>) and Teague et al. (2010).

Leave Early” (“Stay or Go”), was developed and adopted in light of policy revision after the major bushfires in South Australia in 1983. The overarching principle of Stay or Go empowers individuals households with decisions about whether to stay and defend properties or evacuate in advance of wildfires (Taylor & Freeman 2010). The Stay or Go approach depends upon self-reliance rather than central authority. It leaves households with the ultimate decision about how to respond, but assigns fire agencies the responsibility to provide households with means for making this decision, such as increasing people’s knowledge of bushfire risk (McLennan & Handmer 2012).

The policy stresses a requirement that people choosing to stay and defend must be properly equipped and physically and mentally prepared to do so. Those choosing this option also assert a commitment to staying at home until the fire passes, understanding that leaving once a fire is nearby is most dangerous and assistance from emergency responders is likely not possible. Guidelines suggest how a property must be defended, such as preparing property through fuel management, undertaking house protection measures, and ensuring that household members possess sufficient resources to actively defend property (Taylor & Freeman 2010). The Stay or Go policy does not encourage people to passively “shelter in place” (Stephens et al. 2009). (In the United States, the phrase “shelter in place” in the context of fire implies a more passive response than the Australian directive, which centers on active defense of property (Stephens et al. 2009).) It is dangerous to choose to stay but later panic and attempt to self-evacuate or request evacuation assistance from others (Taylor & Freeman 2010). In fact, prior to Black Saturday, most civilian deaths in bushfires in Australia were the result of the choice to evacuate late (Teague et al. 2010).

Official policy about defending one’s property during a bushfire was devised based on evidence that well-prepared homes can provide a safe place for people during wildfires; a firebreak typically passes quickly, and a house can survive this short period and protect occupants from radiant heat, smoke, and embers. Furthermore, the spread of fire from embers can be reduced if residents are present, prepared, and actively defending a property against fire.

**16.3.2.2 Incident Command** The state of Victoria’s emergency management framework shown in Figure 16.3 provides for planning, preparation, and coordination in the management of crises and natural disasters. On Black Saturday, the Country Fire Authority (CFA) and Department of Sustainability and Environment (DSE) were colocated and operating (for the first time) from the integrated Emergency Coordination Centre (iECC) in Melbourne. The purpose of the iECC was to achieve effective strategic planning and coordination, better information sharing, and faster decision making (Teague et al. 2010). Despite attempts to coordinate agencies, the CFA and DSE followed operating procedures that were not consistent, used incompatible technology systems, and often duplicated functions; consequently, true integration was not achieved (Teague et al. 2010). There was no single agency or individual in charge of operational planning, tasking, and accountability. Responsibilities were divided between the CFA’s chief officer, DSE’s chief fire officer, the chief commissioner of police, and the emergency services commissioner.



**FIGURE 16.3** Emergency response structure. Adapted from (<http://blacksaturdayfires.wikispaces.com/Timelines>) and Teague et al. (2010).

The CFA and the DSE were responsible for the prevention and suppression of fire. The chief commissioner of police was responsible for coordination across agencies and managing public warnings. The emergency services commissioner acted as advisor and kept the minister for police and emergency services informed (Teague et al. 2010).

Despite the best efforts of many in the CFA and DSE—and a memorandum of understanding promoting cooperation—the two agencies' systems were not aligned. Information could not always be transferred between the agencies, and nor could emergency workers readily or fully gain access to the other agency's systems. The failings in information sharing and management had severe consequences for people making decisions on the ground at the scene of fires, potentially putting lives at risk. For example, there was duplication of resources between the CFA and DSE in mapping, IT, information systems, and manual uploading of warning information, contributing to a lack of information collection, analysis, and dissemination. This led to weaknesses in public bushfire warnings and contributed to some warning delays (and even failure to issue warning). In the Murrindindi fire, for example, the response was

managed from two separate facilities in the same town, without coordination between the DSE and CFA teams (Teague et al. 2010). Furthermore, too much emphasis was devoted to fire suppression and not enough to public information such as wind change advice, warnings to the public, and updates provided to the iECC (Teague et al. 2010). Although the minister for police and emergency services acted properly before and during the bushfires, the ministry should have introduced the option of declaring a state of disaster with the premier of Western Australia, as the bushfire conditions met the criteria for consideration (Teague et al. 2010). Such a declaration would have acknowledged the gravity of the situation and elevated focus on community safety and warnings.

**16.3.2.3 Local Government Preparedness and Response** At the local level, the performance of individual Incident Management Teams (IMTs) varied. IMTs that were well prepared and staffed by workers with appropriate training and experience managed difficult fires well; at the same time, problems arose at IMTs that were poorly prepared or did not have access to fully qualified staff. The greatest difficulties arose in managing information flows, which are critical for issuing public warnings and informing firefighters of changing conditions and potential danger (Teague et al. 2010).

Police and local councils also reported communication problems stemming from a lack of information flowing from Incident Control Centers (ICC). Among the concerns expressed were difficulties obtaining information about the location and spread of fires and about the location of roadblocks. A lack of information also created difficulties for police and municipal emergency coordination centers and affected decisions about deployment of resources and advice to residents (Teague et al. 2010).

Firefighting support itself was provided through cooperation between public entities (firefighters [from within Australia and abroad], industry brigades, police, ambulance, and emergency service workers) and private operators (private units and volunteers). This diversity of firefighting workforce is a practical and valuable expression of shared responsibility that strengthens the state's overall firefighting capacity (Teague et al. 2010). The strength of the CFA volunteer base was particularly evident, including its surge capacity, the local knowledge of its members, and its rapid response. There was anecdotal evidence of volunteers' preparedness and response efforts, such as warning local residents and assisting with the task of locating and identifying the deceased. Private units, typically operated by farmers or landowners employing their own firefighting equipment, also played an important role in firefighting in many parts of Victoria.

### **16.3.3 Evacuation Policy**

The evacuation policy in place in Victoria on February 7, 2009, reflected a national policy implemented by all fire agencies in Australia and outlined in a 2005 statement by the Australasian Fire and Emergency Service Authorities Council (AFAC) (Australian Fire Authorities Council 2005). With regard to evacuation, the key elements of AFAC's (2005) position were that last-minute evacuations are dangerous; that

large-scale evacuation is generally not the preferred option; that with adequate preparations, it is better for people to remain at their homes than to evacuate; and that prepared people should not be forcibly removed from their properties. The policy suggested that the main priority of fire agencies is to control the fire through suppression, protect property, manage roadways, and advise the public on appropriate precautions (as opposed to dictating specific actions). These actions were considered optimal in protecting human life and considered both the safety of the firefighters and the public (McLennan & Handmer 2012).

The State Emergency Response Plan places the decision to issue a mandatory evacuation order with the Incident Controller. On Black Saturday, in accordance with agency practice, Incident Controllers did not consider evacuation of any municipalities affected by the fires. Local police, Victoria State Emergency Services (VICSES), and firefighters did, however, initiate *ad hoc* arrangements to evacuate some areas, including vulnerable populations, with little input from IMTs. Many residents made the decision (either on their own or on the advice of emergency workers) to evacuate, traveling out of affected towns or to places of refuge within towns (Teague et al. 2010).

**16.3.3.1 The Decision to Evacuate** Individual and household decisions to evacuate or not evacuate are complex. Various issues contribute significantly to evacuation behavior: a lack of warnings and weak buildings, household connections to place, and the psychology of engaging with fire risk (O'Neill & Handmer 2012). First, from an emergency management perspective, decision making did not adapt when risk increased. For example, although the state premier and chief fire officer warned that the fire danger index on Black Saturday would likely reach the highest on record, fire management procedures were elevated only minimally beyond normal practice for an extreme weather day (O'Neill & Handmer 2012). Residents appeared to expect a warning directly from a government official about the fire, but in fact, only 9% of those who perished in the fire received such specific warnings. This meant many people were taken by surprise by the fire or failed to fully implement their fire defense plans (O'Neill & Handmer 2012).

For residents, bushfire preparedness requires awareness of fire risk and knowledge of what to do in an event; however, in cases of fatalities, 25% did not have a general awareness that they were located in a bushfire risk area, 39% lacked basic knowledge of how to mitigate fire risk, and less than 50% had made a fire plan. Fire plans that did exist varied in quality, and there was no evidence that households made contingency arrangements in case their plan could not be executed (O'Neill & Handmer 2012).

The results of a survey of residents by Teague et al. (2010) showed that of those who left, 32% (and many of these with children) departed more than 2 hours before the fires arrived in their towns. In addition, 53% of residents left less than an hour before the fire arrived, and 75% of those who decided to initially stay, but evacuated at some stage during the fires, left when the fire reached within one-third mile (500 m) of their property (Teague et al. 2010). Considerable numbers of people survived by leaving their homes shortly before the fires arrived and in some cases successfully left areas where nearly all who stayed died. There were also a number of people who

died while fleeing—in these cases, the decision was made so late that the only option left was to try to outrun the fire.

Twenty-four people died fleeing in vehicles or on foot (Teague et al. 2010). Radiant heat is extremely unsafe and more dangerous than it appears, and fleeing on foot is often deadly (Taylor & Freeman 2010). Likewise, driving is dangerous because smoke can reduce visibility and increase the risk of a crash for panicked drivers in stressful situations. Cars are not safe from radiant heat. Furthermore, closed roads can cause drivers to turn away from a planned evacuation route, leaving less time to escape the firefront.

An example of an impromptu but orderly mass evacuation occurred in the town of Marysville. Police officers, realizing there was a pressing need to evacuate quickly, directed 200 people in 60 cars and other vehicles who had gathered at a preplanned location to drive in convoy to Alexandra. This approach defied prevailing policy, but officers were confident that evacuation was possible because they had recently traveled on passable roads nearby. The evacuation was described as calm and orderly and the convoy reached Alexandra safely. Volunteers in two VICSES vehicles drove along the streets of Marysville to sound warnings to any residents remaining in the town; the volunteers used the public address system in the VICSES vehicles and visited homes door-to-door advising all vehicles evacuating Marysville to go to Alexandra (Teague et al. 2010).

*Vulnerable Populations* Populations living in fire-prone areas may be particularly vulnerable if they lack basic knowledge of fire, have low levels of preparedness, or have physical or mental disabilities (O'Neill & Handmer 2012). In the case of Black Saturday, some vulnerable residents who remained in the fire area died: 44% of all fatalities occurred among vulnerable people due to age (12 years or younger, 70 years or older) and/or chronic and/or acute disabilities (Teague et al. 2010). Although the idea of responsibility sharing with those at risk has been part of the bushfire policy in Australia, in the case of Black Saturday, greater responsibility and therefore greater risk were placed on individuals and households, even though much of the population was particularly vulnerable due to age, disability, or risky location. Another factor influencing vulnerability was the potential defense of homes. Forensic experts questioned whether the buildings occupied by 32% of those who died were actually defendable (O'Neill & Handmer 2012).

*Hospitals* Two organized institutional evacuations occurred on Black Saturday. The Bunyip Hillview aged care facility and Neerim Hospital were evacuated at the discretion of staff members, who, after assessing the risk of the Bunyip fire, notified the Department of Human Services and the Municipal Emergency Response Coordinator about a need for facility evacuations. In the Hillview case, MERC advised the facility's CEO to begin an evacuation and arranged for VICSES volunteers, a bus, and ambulance transport for those who required it. The hospital evacuation proved challenging, however, due to insufficient coordination and inadequate transportation (Teague et al. 2010).

### 16.3.4 Black Saturday Tests Stay or Go Policy

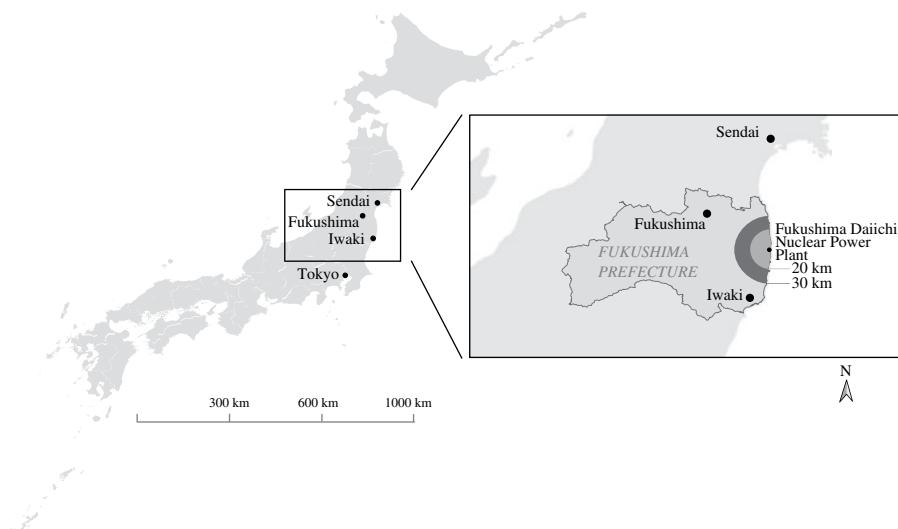
The severity of the Black Saturday fires exposed weaknesses in Victoria's emergency management structure and Stay or Go policy. First, Teague et al. (2010) found that the policy failed to allow for different preparedness and response measures depending on variations in fire severity. For example, if the fire is too intense to be contained, focus should switch to community safety rather than fire suppression. Second, the focus of the warnings issued was too narrow. The Stay or Go policy operates under the assumption that individuals and households have a fire plan, but many people did not have effective plans. When it came time for individuals and household to make the decision to evacuate or not to evacuate, citizens received inadequate guidance from authorities. In other words, warnings were directed at getting people to enact their fire plans, rather than giving more specific directions or advice (since not everyone had a fire plan). Further, rather than leaving early as recommended, people had a tendency to wait and see. For those people, fallback alternatives—the organized execution of large-scale evacuations and the provision of shelters—were lacking. The shortcomings experienced during Black Saturday could be addressed if emergency managers provide more options and different advice. Third, the policy and accompanying educational materials and advice were lacking in important ways. Inadequate information was provided to citizens about several key knowledge areas: fire behavior, the difficulty of making a property defendable, the risks inherent in defending a house, the fact that vulnerable people (including children) should not be present, and that firefighting equipment must be resilient. Finally, within state-level emergency management practice, there was confusion about responsibilities and important deficiencies of leadership.

Following Black Saturday, US fire officials abandoned consideration of a modified Stay or Go approach and began emphasizing evacuation as the safest choice for all situations (Paveglio et al. 2012). Likewise, in Australia, there has been a shift in emphasis away from self-reliance of individuals and communities (especially where vulnerable populations are concerned) toward a greater degree of responsibility for emergency service leaders (McLennan & Handmer 2012). There has also been greater attention to responsibility sharing for bushfire risk management (McLennan & Handmer 2012) and efforts to better understand the difference between good intentions and appropriate action through greater preparedness in risk areas (Whittaker & Handmer 2010).

## 16.4 CASE 2: MULTIHAZARDS STRIKE SEQUENTIALLY AND WITHOUT WARNING IN JAPAN (2011)

### 16.4.1 Disaster Overview

The nuclear disaster caused by the Fukushima Daiichi Nuclear Power Plant (FDNPP), owned and operated by the Tokyo Electric Power Company (TEPCO), was a man-made disaster that the chairman of the Fukushima Nuclear Accident Independent Investigation Commission believes “could and should have been foreseen and prevented” (Kurokawa 2012, p. 9). It is, however, widely accepted that the immediate



**FIGURE 16.4** Study area map.

cause of the nuclear meltdown was the result of two natural disasters. The first was a magnitude 9.0 earthquake with an epicenter in the Tōhoku region of Japan, 161 kilometers (100 miles) northeast of FDNPP, which took place on March 11, 2011. The earthquake triggered an automatic emergency shutdown of FDNPP Units 1, 2, and 3; Units 4, 5, and 6 were already in cold shutdown. At that time, there was no severe loss of safety functions (Thielen 2012).

The earthquake triggered a second natural disaster—a powerful tsunami—approximately 1 hour later. A 14 m (46 ft) wave—8.2 m (27 ft) higher than the maximum safety level—reached FDNPP causing severe flooding; damage to buildings, equipment, and machinery; blockage of water intake buildings; and the loss of emergency diesel generators and eventually the loss of all electrical systems, known as station blackout. As a result, there was a complete loss of cooling of the reactor cores of Units 1, 2, and 3, as well as of the fuel element pools of Units 1 through 6 (Thielen 2012). Exacerbating the problem was road damage caused by the earthquake and tsunami, which made it difficult to reach FDNPP from the outside. The massive release of radionuclides into the atmosphere and the Pacific Ocean led to a declaration of a Level 7 (severe) accident on the International Nuclear Event Scale (INES) (Thielen 2012). Monitoring suggested that the radiological situation for people in Japan was very serious but regionally limited (Thielen 2012); therefore, it is the region around FDNPP depicted in Figure 16.4 and the government's and citizen's immediate response to the disaster that are the foci of this study.

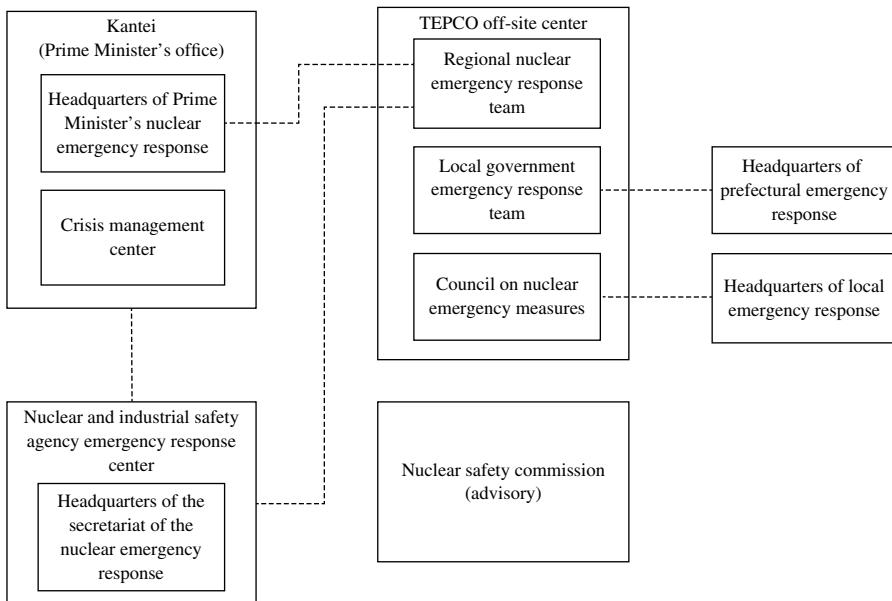
#### 16.4.2 Emergency Preparedness and Response

According to the Fukushima Nuclear Accident Independent Investigation Commission (Kurokawa 2012), failures of the chain of command in responding to the emergency existed at all levels: from TEPCO management, all the way to the *Kantei*, the office

of the prime minister. Overall, systems that had been planned for use in a disaster—such as communication and transportation infrastructure—were disabled by the tsunami and the earthquake. Furthermore, the failure of the government's emergency response system to function from the very beginning caused the *Kantei* to increase its involvement in the response to the accident, which ultimately contributed to confusion and ineffectiveness (Kurokawa 2012).

**16.4.2.1 Failures in Chain of Command** Failures in the chain of command began immediately following station blackout. TEPCO's chairman and president had different understandings of the emergency response structure, which likely contributed to the delay in TEPCO's response to the accident. TEPCO's written manual for emergency response, which relied on monitoring unable to be performed due to electricity loss, was largely ineffective. Finally, TEPCO's head office did not offer sufficient technical support. Most importantly, there was reluctance to issuing a full withdrawal of the plant itself both from the *Kantei* and TEPCO (Kurokawa 2012).

If disaster strikes, TEPCO management should communicate with the Nuclear and Industrial Safety Agency (NISA)—depicted in Figure 16.5—through the off-site Emergency Response Center (ERC). This was not possible as the off-site center was powerless from earthquake damage. The main agencies responsible for the government's accident response system are the prime minister's Nuclear Emergency Response Headquarters and its secretariat and the Regional Nuclear Emergency Response Team. Neither of these organizations functioned as planned. The prime minister's Nuclear Emergency Response Headquarters and its secretariat are responsible for the overall



**FIGURE 16.5** Japan nuclear emergency response structure. Adapted from Kurokawa (2012) and Hatamura (2012).

coordination of emergency response measures, such as deciding how to protect nearby residents, but they were unable to carry out these functions primarily due to communication lapses (Kurokawa 2012). Additionally, the Regional Nuclear Emergency Response Team did not initiate a local response to the accident—such as issuing an evacuation order—because of its preoccupation with relief demand associated with the earthquake and the tsunami. Likewise, the Crisis Management Center, located in the *Kantei* building, was unable to respond appropriately to the nuclear accident. Other disaster response players such as the Nuclear Safety Commission and the Ministry of Education were unable to share their expertise in the situation (Kurokawa 2012).

Further confusing the chain of command was the prime minister's decision to go to FDNPP and take command when the government's main responsibility should have been to the public. This caused a disruption in TEPCO's planned chain of command, the regulatory agencies, and the prime minister's office. Therefore, as the situation deteriorated and planned government accident response systems failed to function, control of emergency response was assumed by the *Kantei*, with the prime minister at the center of an impromptu group of politicians, advisors, and the chairman of NISA. This group included people who were not emergency experts and lacked adequate understanding of the on-site situation (Kurokawa 2012).

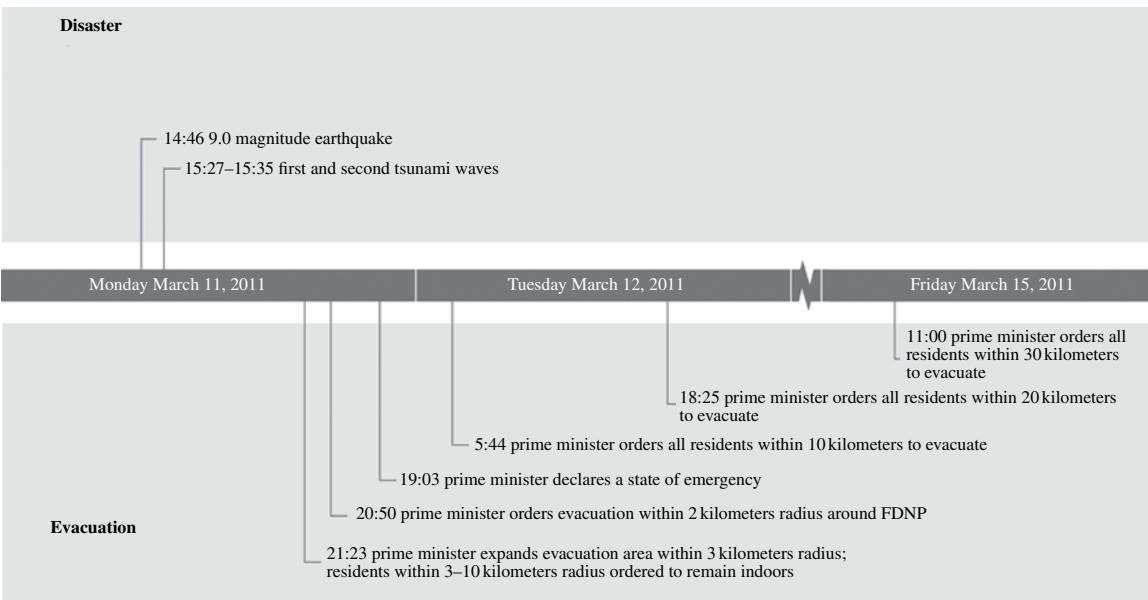
The prime minister's office effectively became the front line for disaster response. After the *Kantei* was notified by TEPCO that the situation at FDNPP met the conditions of Article 15 of the Act on Special Measures Concerning Nuclear Emergency Preparedness (1999), it took 2 hours to issue the Declaration of a Nuclear Emergency Situation—a necessary step in initiating the emergency response. The prime minister's office was also central in decisions regarding the evacuation zones. The secretariat of the Nuclear Emergency Response Headquarters should have been responsible for drawing up evacuation proposals; because the secretariat was delayed due to the natural disasters, however, the *Kantei* stepped in and ordered the evacuations. Consequently, decisions were made on an ad hoc basis; there was insufficient cooperation between the governmental agencies; there was a deficiency in the details of evacuation operations; and there was a lack of suitable explanation to the public. This led to escalating disorder and confusion on the ground (Kurokawa 2012).

### 16.4.3 Evacuation Procedures

**16.4.3.1 Evacuation Orders** Following a declaration of a state of emergency, evacuation orders based on radial distance from FDNPP were revised five times in 24 hours (see Fig. 16.6) by the prime minister, according to the escalation of the accident situation. Three reactors experienced fuel core meltdowns, and three of the reactor buildings' roofs and walls were destroyed in hydrogen explosions during a 3-day period, increasing the intensity of the disaster. By March 16, 12 municipalities had executed a full-scale evacuation (Kurokawa 2012; Kushida 2012).

#### 16.4.3.2 Local Government Preparedness and Response

*Prefecture Government and Local Municipalities* Both the Act on Special Measures Concerning Nuclear Emergency Preparedness (1999) and Basic Law on Emergency



**FIGURE 16.6** Timeline of events in Japan. Adapted from Kushida (2012) and Nishino et al. (2012).

Preparedness (2000) state that local public entities are required to establish procedures to both prevent a nuclear emergency and respond to an emergency nuclear situation. In response to these various ordinances, the Fukushima Prefecture did possess a disaster prevention plan (Hatamura 2012). This plan, however, did not take into account the possibility of a nuclear disaster caused by concurrent natural disasters nor a breakdown in communication from the central government. Because of this, in an act of desperation, the Fukushima Prefecture unilaterally ordered that residents within a 2 kilometers (1.3 miles) radius of the plant be evacuated, according to established procedure. This was followed 30 minutes later by the prime minister ordering an evacuation of residents within a 3 kilometers (1.9 miles) radius (Kurokawa 2012).

Municipalities within 8 to 10 kilometers (5 to 6.2 miles) of a nuclear power station are also required to develop nuclear disaster prevention and response plans (Nishino et al. 2012). The following sequence of events is usually included in such a plan: a municipality decides to carry out a full-scale evacuation resulting from an order by the prime minister or based on independent judgment; the municipality requests from nearby municipalities sheltering for its residents; the municipality issues an evacuation order and communicates with residents; the municipality ensures vehicles to transport residents either through its own resources or by receiving support from the Prefecture or another governing body; and the municipality organizes gathering points where residents can acquire transport to designated sheltering municipalities (Nishino et al. 2012).

*Communication with Evacuees and Public Reaction* In addition to failures in the chain of command, there were significant failures in the communication system resulting in ineffective information sharing and communication of evacuation orders. It is well documented that the earthquake and tsunami had seriously damaged the emergency communication infrastructure, making it difficult to transmit the evacuation order to local municipalities through customary communications channels. Although there was a teleconference system connecting the *Kantei* and each disaster management organization, there is no evidence that the system was used for sharing information. TEPCO had brought its own teleconference system to the off-site center and used it to connect with the plant in Fukushima, but it was not connected to the governmental teleconference system, which, had a connection been established, could have potentially allowed for more effective information sharing between all the parties involved in the early stages of the emergency (Kurokawa 2012).

The central government was not only slow in informing municipal governments about the nuclear power plant accident but also failed to convey the severity of the accident (Kurokawa 2012). Most municipalities learned of the evacuation orders through mass media (likely television) at the same time as citizens (Hatamura 2012). In turn, the cities, towns, and villages communicated with citizens in the area by using a municipal disaster management radio communication network, sound trucks, and police cars and by fire fighters making door-to-door visits. The problem with the lack of communication coordination and the use of these informal systems was that many residents in the plant's vicinity evacuated without accurate information and instructions.

Similarly, the speed with which information traveled varied significantly depending on the distance from the plant. In a survey of evacuees, Kurokawa (2012) found that only 20% of the residents closest to the plant knew about the accident when evacuation from the 3 kilometers (1.9 miles) zone was ordered. Furthermore, the survey found that most residents within 10 kilometers (6.2 miles) of the plant learned about the accident more than 12 hours after the Article 15 notification (Act on Special Measures Concerning Nuclear Emergency Preparedness 1999), but received no further explanation of the accident or evacuation directions. As a result, many residents had to flee with only the bare necessities, were forced to move multiple times or to areas with high radiation levels, and were confused by prolonged shelter-in-place orders or voluntary evacuation orders (Kurokawa 2012).

The Fukushima Prefecture also was unable to effectively conduct nuclear monitoring—a major component of nuclear disaster planning. Some residents were evacuated to high-dosage areas because radiation monitoring information was not collected or provided to residents. Some people evacuated to areas with high levels of radiation and were then neglected, receiving no further evacuation orders until April 2012 (Kurokawa 2012). Kurokawa (2012, p. 38) argues that “the government effectively abandoned their responsibility for public safety.” Approximately 70% of the residents of Futaba, Okuma, Tomioka, Naraha, and Namie had to evacuate four times or more because of insufficient monitoring and confusing evacuation orders (Kurokawa 2012).

Evacuation procedures were further complicated by residents’ delays in initiating evacuation behaviors (Urata & Hato 2012). Generally, people make decisions during disasters based on information available through the mass media and community networks about the potential danger and based on their ability to self-evacuate (e.g., ability to travel, dependence on others). The success of large-scale evacuation frequently relies on cooperation behaviors among residents—for example, information exchange about dangers, safe places, and mutual assistance, particularly to aid individuals with low mobility (Urata & Hato 2012). It is evident that in the FDNPP scenario, cooperation was inadequate.

#### **16.4.4 Local Evacuation**

A total of 146,520 residents were evacuated as a result of mandatory governmental evacuation (Kurokawa 2012). Most residents rushed to leave by car or by buses chartered by the government (Tanigawa et al. 2012). In advance of the evacuation orders, Crisis Control Center anticipated that a mandatory evacuation of residents might be required and requested the Passenger Transport Division of the Automobile Bureau of the Ministry of Land, Infrastructure, Transport and Tourism to charter approximately 100 buses for evacuation. The Passenger Transport Division was responsible for coordinating this effort with the prime minister’s office and the Crisis Control Center. The bus companies in the Tohoku and Kanto areas were charged with organizing vehicles (Hatamura 2012). The Passenger Transport Division was not included on the list of relevant ministries required to respond in the event of a nuclear hazard. Consequently, the Passenger Transport Division had never participated in a nuclear emergency drill or exercise (Hatamura 2012).

In response to the evacuation order issued at 5:44 a.m. on March 12, buses were used for the evacuation of residents in the area within a 10 kilometers (6.2 miles) radius of the FDNPP. The buses that had been organized were gathered in a designated location in the town of Okuma and were assigned to the municipalities located in the evacuation zone by the Local Nuclear Emergency Response Headquarters staff. However, since there were not enough staff assembled at the Local Nuclear Emergency Response Headquarters, the buses were not allocated efficiently (Hatamura 2012). In addition, since roads were damaged by the earthquake and streets were congested with evacuation vehicles, the number of buses dispatched to the municipalities was inadequate (Hatamura 2012).

**16.4.4.1 Local Evacuation in Detail** The following sections describe two specific evacuation cases: (i) the town of Futaba and (ii) the town of Tomioka (with the village of Kawauchi).

- *Futaba*

Following the tsunami, Futaba residents first evacuated to shelters within the town. When Futaba was included in the FDNPP evacuation zone, residents moved north to the town of Namie. Soon after evacuees arrived, Namie itself was designated an evacuation area, and evacuees moved to the town of Kawamata, about 40 kilometers (24.9 miles) northwest of Futaba. In Kawamata, Futaba residents were divided among seven shelters, and about 1500 of Futaba's 6500 residents were transported a total of 200 kilometers (124 miles) in 40 buses (the rest of the residents remained in Kawamata) to a location in which they could live together—an event facility in the city of Saitama. The facility became unavailable at the end of March 2012, and about 1200 people and local government officials evacuated again to a neighborhood school. As of April 2012, Futaba was still inhabitable because of high radiation levels; about 300 people still lived in the high school (Urata & Hato 2012).

- *Tomioka and Kawauchi*

When the town of Tomioka was ordered to evacuate, local government communicated messages through the community wireless system used to transmit emergency information. Tomioka's residents were accepted by the village of Kawauchi, located west of Tomioka. Approximately 6100 of the 16,000 residents in Tomioka were evacuated to Kawauchi in personal cars and eight buses. Most evacuees traveled by car, causing severe traffic congestion. Soon after Tomioka residents arrived in Kawauchi, the village was ordered to evacuate. Evacuees chose to shelter in an event facility in the city of Koriyama because of its large size, number of parking spaces, and capacity to receive aid. The group later borrowed land in the same city and built a temporary local government office, which it continues to operate (Urata & Hato 2012).

**16.4.4.2 Vulnerable Populations** A lack of preparedness for vulnerable populations in disaster response has received great attention since Hurricane Katrina (Hess & Arendt 2006; Hess & Arendt 2009). In a study in Japan, Shrader-Frechette (2012)

found that a disproportionate number of poor people, *buraku* (blue-collar workers), and children lived in the vicinity of FDNPP. Economic hardship forced these poorer towns to accept reactors in exchange for funding for basic services without fully understanding the risks. In other words, people who lived near FDNPP bore both higher preaccident and postaccident risks; meanwhile, relatively wealthier Tokyo residents—225 kilometers (140 miles) away—received virtually all FDNPP electricity, yet virtually no environmental injustice or disaster-related environmental injustice. In the end, the Japanese government endangered vulnerable populations living near FDNPP by weakening radiation standards and suppressing information about radiation risks preaccident while also failing to adequately assist or evacuate children and poor people living near the plant postaccident (Shrader-Frechette 2012).

**16.4.4.3 Hospitals** In Japan, emergency evacuation plans for residents within an 8 to 10 kilometers (5 to 6.2 miles) radius around a nuclear power plant is mandated; however, no specific plans for hospital or nursing facilities had been established at the time of the FDNPP disaster (Tanigawa et al. 2012). Before the earthquake and tsunami, eight hospitals caring for 1240 patients and 17 nursing facilities caring for 980 patients were located within a 20 kilometers (12.4 miles) radius of the FDNPP. While the evacuation of hospital inpatients had begun, by the evening of March 13, 2012, it was estimated that 840 patients in hospitals or nursing care facilities remained within a 20 kilometers (12.4 miles) radius of the plant (Tanigawa et al. 2012). The following day, when the prime minister ordered emergency evacuation for all patients in the area, the result was a hurried relocation of these patients to Minamisoma, a city 26 kilometers (16.2 miles) northwest of the plant.

As the situation at the damaged plant became more volatile, hospital evacuations became more rushed. Patients were transported by police vehicles packed full with both patients and other residents who had not previously evacuated. Medical personnel did not accompany the patients during evacuation, and bedridden patients were laid down on seats causing some patients to fall. When no admitting hospitals or facilities could be found and vehicles were required elsewhere, patients were temporarily housed at shelters with no heat or medical supplies (and some waited for more than 24 hours before reaching admitting facilities, resulting in deterioration of the physical condition of many patients) (Tanigawa et al. 2012). In studying the evacuations of hospitals following the FDNPP disaster, Tanigawa et al. (2012) suggest that detailed evacuation plans for these vulnerable populations are imperative and should include such information as the distribution of hospitals and nursing facilities, number of patients, available vehicles, accompanying medical personnel for transportation, evacuation routes, and estimated duration for evacuation.

Hospitals and nursing homes in the 20 kilometers (12.4 miles) disaster zone struggled to secure evacuation transportation and find accommodations for patients, contributing to the deaths of 60 patients in March 2012 (Hatamura 2012). At Futaba Hospital, the evacuation of bedridden patients was delayed by several days after the evacuation order was called (Hatamura 2012). When patients were evacuated, the sheltering location was a school gymnasium in a remote location. Challenges stemmed from a lack of preparedness. For example, the Prefecture disaster plan was ambiguous about

which organization was actually responsible for evacuating hospitals and nursing facilities. When the transportation support squadron of the Ground Self-Defense Force began evacuating patients, it did not have any means of communicating with its command center.

**16.4.4.4 Facilities for Older Adults** Like hospitals, no specific plans were included for older adults in institutions (Yasumura et al. 2012). Among the evacuees in the designated evacuation zone, there were 1770 institutionalized older adults at 34 community facilities. The government arranged transportation, and transfers began on March 12, 2012—relocating the elderly to hospitals, municipal gymnasiums, and public schools. These residents could not take any personal belongings (including clothing) because of limited space, and many were transferred several times to various locations in the following months. Evacuees were required to present “radiation-free” certificates to the shelters, or they were refused entry (Yasumura et al. 2012).

The impact of a disaster on the excess mortality of institutionalized older adults was most significant in the immediate aftermath, but also had a lasting impact due to diminished nutritional, hygienic, medical, and general conditions (Yasumura et al. 2012). This finding of excess mortality reflects the vulnerability of the institutionalized elderly to change and a need for special attention and care of this subpopulation in disaster evacuation.

#### 16.4.5 Emergency Preparedness Failures Threaten Public Safety

Several key factors contributed to the many failures in regard to TEPCO and the Japanese government’s reaction to the FDNPP disaster. First, Acton and Hibbs (2012) found that the FDNPP accident was man-made and likely preventable. The disaster resulted from failures in regulation and nuclear plant design upgrades and especially misjudging the risk from tsunamis—both are operational aspects in which FDNPP lagged behind international best practices and standards.

Second, there were numerous reports of failures in communication systems at all levels stemming from the two natural disasters that jeopardized planned systems causing the chain of command to perform ineffectively in responding to the incident. This reveals a lack of resiliency and redundancy where emergency communication and technology is concerned.

It was also well documented that preparedness measures were greatly lacking. In terms of resident preparedness, fewer than 15% of residents in the evacuated towns reported receiving evacuation training for a nuclear disaster, and fewer than 10% of residents reported receiving information about the possibility of a nuclear accident (Kurokawa 2012). Activities to raise public awareness are needed to provide residents with basic knowledge of how radioactive substances are released and dispersed into the atmosphere and how exposure to radiation can affect health (Hatamura 2012).

Local government bodies should improve evacuation readiness plans as well. Hatamura (2012) suggests periodically conducting evacuation drills and promoting resident participation in such drills. Other preparedness measures include ensuring

access to transportation, establishing evacuation sites in outlying areas, and ensuring water and food supplies in places of refuge, knowing that the evacuees may number in the thousands or tens of thousands. Furthermore, disaster plans should better consider the evacuation of vulnerable populations living at home or in institutions such as hospitals or nursing homes. Finally, due to the large area affected by nuclear disasters, local municipal governments should work together with prefectural and national governments in developing disaster readiness plans (Hatamura 2012).

## 16.5 SYNTHESIS AND CONCLUSION

In two detailed cases, we explored the outcomes of mandatory and nonmandatory evacuation related to no-notice and limited notice disasters in nonurban settings. We find value in investigating a no-notice event (earthquake) and a limited notice event (wildfires) because the findings can be extended to other settings and disaster types. The research produces three key findings about emergency preparedness, response, and evacuation procedures.

- a. **Jurisdictional and interorganizational complexity complicates emergency response in the event of a disaster, especially in the case of a “double” or “triple” event (as was the case in the FDNPP disaster) or if a disaster’s magnitude stretches beyond what is anticipated (as was the case on Black Saturday).**

The challenges of interjurisdictional collaboration are twofold (Hess et al. 2013b). A first challenge is a need for more clearly defined intergovernmental relationships and processes (Renne et al. 2009). In the case of the FDNPP disaster, the main agencies responsible for the governmental nuclear accident response system did not function as planned because of technological breakdowns and preoccupation with responding to the preceding earthquake and tsunami. The failure of the government’s emergency response system to function effectively from the beginning caused the *Kantei* to increase its involvement in the response to the accident, which ultimately heightened confusion and ineffectiveness (Kurokawa 2012). The distribution of responsibilities and resources in disaster response can become hindered when the local structure of coordination and command are disrupted by state and federal response (Renne et al. 2009).

A second challenge is the need for improved coordination among first responder agencies (Renne et al. 2009). For example, during the 2009 bushfires in Victoria, despite the best efforts of many in the CFA and DSE, the two agencies’ systems were poorly aligned. Information could not be efficiently transferred between the agencies, nor could emergency workers readily or fully gain access to the other agency’s systems. The failings in information sharing and management had severe consequences for people making decisions on the ground at the scene of fires, potentially putting lives at risk (Teague et al. 2010). Improving interjurisdictional collaboration through disaster preparedness

efforts—by establishing improved protocols, training, and communication—may be the most effective way to increase the effectiveness of disaster response (Hess et al. 2013b).

- b. **An effective emergency response system must have resilient methods of communication and consistent messaging, as communication is often the first system to break down in the chaos of an extreme event.**

Properly planned communications systems allow for the movement of information seamlessly between command units and their subsidiary entities, as well as among collaborating agencies and organizations. The most successful communications and information systems used in emergency management are designed to be flexible, reliable, and scalable in order to function in any type of disaster, regardless of cause, size, location, or complexity. Communication systems should be suitable for operations within a single jurisdiction or agency, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement, allowing various personnel to maintain a constant flow of information during an incident (Department of Homeland Security 2008).

Communication weaknesses were prevalent in the case studies in both Australia and Japan, plaguing higher levels of governmental decision making and leading to confusion on the ground for both emergency workers and the public.

On Black Saturday in Australia, police and local councils reported communication problems stemming from a lack of information flowing from ICC. Among the concerns expressed were difficulties obtaining information about the location and spread of fires and about the location of roadblocks. A lack of information also created difficulties for police and municipal emergency coordination centers and affected decisions about deployment of resources and advice to residents (Teague et al. 2010). Likewise in Japan, the central government was not only slow in informing municipal governments about the nuclear power plant accident but also failed to convey the severity of the accident (Kurokawa 2012). Most municipalities learned of the evacuation orders through mass media outlets such as television news at the same time as citizens (Hatamura 2012).

Public messaging was also a problem in both international disasters. In Japan, for example, a series of announcements that widened the evacuation zone (from its original size of 2 kilometers (1.2 miles) to its eventual size of 30 kilometers (18.6 miles)) caused uncertainty among residents about whether or not they should evacuate; further confusion stemmed from evacuation orders called by local emergency workers that were not announced through official channels. It is also important to note that when the first evacuation calls were made, the prime minister urged people living within 20 kilometers (12.4 miles) to 30 kilometers (18.6 miles) from FDNPP to stay indoors; however, many people in that zone and even outside of it opted to evacuate making it difficult to transport supplies and assistance to the remaining residents who were sheltering in place (Koyama et al. 2011).

Public messaging on Black Saturday, consistent with the Stay or Go policy in Australia, communicated a message to citizens to take primary responsibility

for their own actions and well-being (and the well-being of their families and property) during disasters. That is, emergency managers were tasked with communicating disaster warnings, but it was ultimately up to individuals to make their own decisions about remaining at home or moving to safety. The Stay or Go message gave residents the option to choose to proactively self-evacuate or adopt a “wait and see” action, and many people, perhaps choosing the path of least resistance—or perhaps experiencing feelings of uncertainty—selected the latter. A clearly communicated mandatory evacuation order, on the other hand, would have required all people to leave, reducing citizen power for extinguishing small fires and defending properties (except for those who break the law by disobeying evacuation orders) but leaving professional crews to better focus on fire safety and not compromise firefighting when called to rescue people in distress.

In addition to clear messaging, this research also emphasizes the importance of redundancy in communication systems, as disasters often cause accidental technological breakdowns due to infrastructure damage or intentional shutdowns as public security measures. To address these challenges, a disaster communication plan should possess multiple channels, including websites, social media, television, radio, print, and smartphones (which can now include image and video content). Available methods for emergency planning officials to communicate with the public have expanded in recent years with the widespread use of smartphones. Emergency planners should continue to produce and refine smartphone apps that provide methods for citizens to both receive information about disasters and to provide information (their whereabouts, assistance needed, etc.). Smartphone apps can be used to link people requesting evacuation assistance with emergency workers (Hess et al. 2013b). Even with these recent technological advances, not everyone has access to all types of technology (especially smartphones), and certain types of disasters may render cellular telephone service unusable; these two points reinforce the importance of both redundancy and clear messaging across all forms of communication.

- c. **While there is a role for oversight of emergency planning for national, state, and local governments, local leaders are best positioned to manage disaster preparedness, response, and recovery—especially drafting evacuation plans and preparing citizens for disasters—as local leaders are best equipped to excel at risk assessment and are more familiar with people, places, and transport routes. Moreover, local leaders are perhaps best positioned to plan for the safety and well-being of vulnerable populations during emergencies.**

Postdisaster evaluations suggest that people near FDNPP were not prepared for an evacuation and that, surprisingly, some people in the vicinity of the nuclear plant did not know the steps to take to prepare themselves and household members for a disaster. Furthermore, large-scale evacuation planning was lacking as evidenced when a large-scale mandatory evacuation was ordered in Japan, but only approximately 100 buses were used for evacuation (more than 100,000 people eventually evacuated), and there was demand for more high-capacity vehicles than there were vehicles available. The Passenger Transport Division

reported that, prior to 2011, it did not undertake emergency drills or exercises. In Victoria, on the other hand, bushfire safety education seemed to be a priority for the state, but materials were designed to prepare Australians for fires that were less disastrous than those experienced in Victoria in 2009—this may have made the Stay or Go policy more palatable than warnings of deadly fires—and thus the severity of the actual disaster exceeded preparation guidance.

Not surprisingly, researchers also found that in the Australia and Japan disasters, emergency managers inadequately preidentified vulnerable populations. In Australia, much could have been done ahead of time to prepare to move people, but in Japan, evacuation orders for the nuclear disaster no-notice event occurred urgently, if at all.

While the earthquake in Japan could not have been stopped by human intervention, the effects of the tsunami on human populations could have been mitigated by adjusting settlement patterns vis-à-vis locations at risk for tsunami inundation. Like the Japan disaster, a certain amount of suffering and loss of life could have been avoided in Australia. The rapidly increasing urban–rural fringe development trend, driven in part by migrant workers and housing affordability, influences the level of risk of bushfires in Australia (Taylor & Freeman 2010); understanding this changing bushsettlement interface is important as planners, elected officials, and emergency management professionals seek to address bushfire safety in the future. In addition, weather experts in Australia predicted with certainty in 2009 that wildfires would be ignited because of extreme heat and favorable fire conditions, and high-capacity transport could have been better prearranged to evacuate everyone in light of elevated risk levels. Where and when possible, emergency managers should stop new populations from locating in disaster zones and relocate population away from disaster zones.

## ACKNOWLEDGMENTS

This research was partially funded by a grant through the U.S.D.O.T./RITA through the University Transportation Research Center—Region II. The authors acknowledge invaluable contributions to the research from Brian Conley, Evan Iacobucci, and Matthew Wattles.

## REFERENCES

- Act on Special Measures Concerning Nuclear Emergency Preparedness. 1999. <http://www.nsr.go.jp/archive/nsn/NSCenglish/documents/laws/8.pdf> (accessed on March 5, 2015).
- Acton, J. M. & Hibbs, M. 2012. *Why Fukushima Was Preventable*. The Carnegies Papers: Nuclear Policy. Washington, DC: Carnegie Endowment for International Peace.
- Australian Fire Authorities Council. 2005. *Position Paper on Bushfires and Community Safety*. Melbourne: Australian Fire Authorities Council.

- Baker, E. J. 1991. Hurricane evacuation behavior. *International Journal of Mass Emergencies and Disasters*, 9(2): 287–310.
- Basic Law on Emergency Preparedness. 2000. <http://www.nsr.go.jp/archive/nsc/NSCenglish/documents/laws/7.pdf> (accessed on March 5, 2015).
- Cameron, P. A., Mitra, B., Fitzgerald, M., Scheinkestel, C. D., Stripp, A., Batey, C., Niggemeyer, L., Truesdale, M., Holman, P., & Mehra, R. 2009. Black Saturday: The immediate impact of the February 2009 bushfires in Victoria, Australia. *Medical Journal of Australia*, 191(1), 11–16.
- Carter, T. M. 1979. *Community Warning Systems: The Interface Between the Broadcast Media, Emergency Service Agencies and the National Weather Service. Report Series 79-02*. Washington, DC: NHWS.
- Cutter, S. L. & Smith, M. M. 2009. Fleeing from the hurricane's wrath: Evacuation and the two Americas. *Environment*, 51(2), 26–36.
- Department of Homeland Security. 2008. *National Incident Management System (NIMS)*. Washington, DC: U.S. Department of Homeland Security.
- Dotson, L. J. & Jones, J. 2005. *Identification and Analysis of Factors Affecting Emergency Evacuations*. Washington, DC: U.S. Nuclear Regulatory Commission, Office of Nuclear Security and Incident Response.
- Elder, K., Xirasagar, S., Miller, N., Bowen, S. A., Glover, S., & Piper, C. 2007. African Americans' decisions not to evacuate New Orleans before Hurricane Katrina: A qualitative study. *American Journal of Public Health*, 97(Supplement 1), S124.
- Fairchild, A. L., Colgrove, J., & Jones, M. M. 2006. The challenge of mandatory evacuation: Providing for and deciding for. *Health Affairs*, 25(4), 958–967.
- Fernandez, M. & Schwartz, J. 2013. Plant explosion tears at the heart of a Texas town. *New York Times*. April 18, 2013.
- Glotzer, D., Psoter, W., Weiserbs, K., & St Jean, R. 2007. The shelter-in-place decision-all things considered. *Australian Journal of Emergency Management*, 22(4), 8.
- Hasan, S., Ukkusuri, S., Gladwin, H., & Murray-Tuite, P. 2011. Behavioral model to understand household-level hurricane evacuation decision making. *Journal of Transportation Engineering*, 137(341), 341–348.
- Hatamura, Y. 2012. *Investigation committee on the accident at the Fukushima nuclear power station. Final Report*. The Cabinet of Japan. <http://www.cas.go.jp/jp/seisaku/icancps/eng/final-report.html> (accessed on March 5, 2015).
- Henstra, D. 2010. Evaluating local government emergency management programs: What frameworks should public managers adopt? *Public Administration Review*, 70(2), 236–246.
- Hess, D. B. 2006. Security on buses and trains: Guarding the Nation's public transit systems against terrorist attacks. *Journal of Security Education*, 1(4), 119–132.
- Hess, D. B. 2007. Floating ramps. *Multi: The Journal of Plurality and Diversity in Design*, 1(1), 8–20.
- Hess, D. B. & Arendt, L. 2006. *Enhancements to Hospital Resiliency: Improving Emergency Planning for and Response to Hurricanes*. Buffalo, NY: Multidisciplinary Center for Earthquake Engineering Research.
- Hess, D. B. & Arendt, L. 2009. *Enhancements to Hospital Resiliency: Improving Emergency Planning for and Response to Hurricanes*. MCEER Technical Report 09-0007. Buffalo, NY: Multidisciplinary Center for Earthquake Engineering Research, University at Buffalo.

- Hess, D. B. & Gotham, J. C. 2007. Multi-modal mass evacuation in upstate New York: A review of disaster plans. *Journal of Homeland Security and Emergency Management*, 4(3), 1–19.
- Hess, D. B., Conley, B. W., & Farrell, C. 2013a. Improving transportation resource coordination for multi-modal evacuation planning: A literature review and research agenda. *Transportation Research Record: Journal of the Transportation Research Board*, 2376, 11–19.
- Hess, D. B., Conley, B. W., & Farrell, C. M. 2013b. *Barriers to Resource Coordination for Multi-Modal Evacuation Planning*. Buffalo, NY: Multidisciplinary Center for Earthquake Engineering Research, University at Buffalo.
- Kaufman, S., Qing, C., Levenson, N., & Hanson, M. 2012. *Transportation During and After Hurricane Sandy*. New York: Rudin Center for Transportation, New York University Wagner Graduate School of Public Service.
- Koyama, A., Fuse, A., Hagiwara, J., Matsumoto, G., Shiraishi, S., Masuno, T., Miyauchi, M., Kawai, M., & Yokota, H. 2011. Medical relief activities, medical resourcing, and inpatient evacuation conducted by Nippon Medical School due to the Fukushima Daiichi Nuclear Power Plant accident following the Great East Japan Earthquake 2011. *Journal of Nippon Medical School*, 78(6), 393–396.
- Kurokawa, K. 2012. *The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission*. Tokyo: The National Diet of Japan.
- Kushida, K. 2012. *Japan's Fukushima Nuclear Disaster: Narrative, Analysis, Recommendations*. Stanford, CA: The Walter H. Shorenstein Asia-Pacific Research Center, Freeman Spogli Institute for International Studies, Stanford University.
- Lindell, M. K., Lu, J. C., & Prater, C. S. 2005. Household decision making and evacuation in response to Hurricane Lili. *Natural Hazards Review*, 6(4), 171–179.
- Mannan, M. S. & Kilpatrick, D. L. 2000. The pros and cons of shelter-in-place. *Process Safety Progress*, 19(4), 210–218.
- McCarthy, F. X. 2011. *Federal Stafford Act disaster assistance: Presidential declarations, eligible activities and funding*. Washington, DC: Congressional Research Service.
- McGuire, M. & Schneck, D. 2010. What if Hurricane Katrina hit in 2020: The need for strategic management of disasters. *Public Administration Review*, 70(Supplement 1), s201–s207.
- McLennan, B. J. & Handmer, J. 2012. Reframing responsibility-sharing for bushfire risk management in Australia after Black Saturday. *Environmental Hazards*, 11(1), 1–15.
- Nishino, T., Ouchi, M., Tsuburaya, S. I., Tanaka, T., & Hokugo, A. 2012. Emergency evacuation of Fukushima residents living in the vicinity of nuclear power station. *Proceedings of the International Symposium on Engineering Lessons Learned from the 2011 Great East Japan Earthquake*, Tokyo, March 1–4, 2012.
- O'Neill, S. J. & Handmer, J. 2012. Responding to bushfire risk: The need for transformative adaptation. *Environmental Research Letters*, 7, 1–7.
- Paveglio, T. B., Boyd, A. D., & Carroll, M. S. 2012. Wildfire evacuation and its alternatives in a post-Black Saturday landscape: Catchy slogans and cautionary tales. *Environmental Hazards*, 11(1), 52–70.
- Rand Corporation. 2007. *Hurricane Katrina: Lessons for Army Planning and Operations*. Santa Monica, CA: Rand Corporation.
- Renne, J. 2006. *Best Practices in Evacuation for the Careless Society*. Working paper. New Orleans, LA: University of New Orleans Transportation Center.

- Renne, J., Sanchez, T., & Litman, T. 2008. National study on carless and special needs evacuation planning: A literature review. *Planning and Urban Studies Reports and Presentations*. Paper 8. New Orleans: University of New Orleans. Transportation Center.
- Renne, J., Sanchez, T., Jenkins, P., & Peterson, R. 2009. Challenge of evacuating the carless in five major U.S. Cities identifying the key issues. *Transportation Research Record*, 2119, 36–44.
- Rittel, H. W. J. & Webber, M. M. 1973. Dilemmas in a general theory of planning. *Policy Sciences*, 4, 155–169.
- Santos, F. & Krauss, C. 2013. Emerging from the rubble in a Texas town. *New York Times*, April 19, 2013.
- Saul, M. H. 2012. Part of New York city evacuated for Hurricane Sandy. *New York Times*, October 28, 2012.
- Shrader-Frechette, K. 2012. Nuclear catastrophe, disaster-related environmental injustice, and Fukushima, Japan: Prima-facie evidence for a Japanese “Katrina”. *Environmental Justice*, 5(3), 133–139.
- Sims, J. H. & Baumann, D. D. 1983. Educational programs and human response to natural hazards. *Environment and Behavior*, 15(2), 165–189.
- Somers, S. & Svara, J. H. 2009. Assessing and managing environmental risk: Connecting local government management with emergency management. *Public Administration Review*, 69(2), 181–193.
- Sorensen, J. H. 1991. When shall we leave? Factors affecting the timing of evacuation departures. *International Journal of Mass Emergencies and Disasters*, 9(2), 153–165.
- Sorensen, J. H., Shumpert, B. L., & Vogt, B. M. 2004. Planning for protective action decision making: Evacuate or shelter-in-place. *Journal of Hazardous Materials*, 109(1), 1–11.
- Stephens, S. L., Adams, M. A., Handmer, J., Kearns, F. R., Leicester, B., Leonard, J., & Moritz, M. A. 2009. Urban–wildland fires: How California and other regions of the US can learn from Australia. *Environmental Research Letters*, 4, 1–5.
- Sternberg, E. & Lee, G. 2009. New York City’s healthcare transportation during disaster: A preparedness framework for a wicked problem. *Prehospital and Disaster Medicine*, 24(2), 95–107.
- Tanigawa, K., Hosoi, Y., Hirohashi, N., Iwasaki, Y., & Kamiya, K. 2012. Loss of life after evacuation: Lessons learned from the Fukushima accident. *The Lancet*, 379(9819), 889–891.
- Taylor, M. A. & Freeman, S. K. 2010. A review of planning and operational models used for emergency evacuation situations in Australia. *Procedia Engineering*, 3, 3–14.
- Teague, B., McLeod, R., & Pascoe, S. 2010. *2009 Victorian Bushfires Royal Commission: Final Report*. Melbourne: Government Printer for the State of Victoria.
- Thames Shipyard and Repair Co. v. United States. 2003. <http://openjurist.org/350/f3d/247/thames-shipyard-and-repair-company-v-united-states> (accessed on March 5, 2015).
- Thielen, H. 2012. The Fukushima Daiichi nuclear accident—An overview. *Health Physics*, 103(2), 169–174.
- Tierney, K., Lindell, M. K., & Perry, R. W. 2001. *Facing the Unexpected: Disaster Preparedness and Response in the United States*. Washington, DC: Joseph Henry Press.
- U.S. House of Representatives. 2006. *A Failure of Initiative: The Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*. Washington, DC: U.S. House of Representatives.

- Urata, J. & Hato, E. 2012. Modeling the cooperation network formation process for evacuation systems design in disaster areas with a focus on Japanese megadisasters. *Leadership and Management in Engineering*, 12(4), 231–246.
- Whittaker, J. & Handmer, J. 2010. Community bushfire safety: A review of post-Black Saturday research. *The Australian Journal of Emergency Management*, 25(4), 7.
- Yasumura, S., Goto, A., Yamazaki, S., & Reich, M. R. (2012). Excess mortality among relocated institutionalized elderly after the Fukushima nuclear disaster. *Public Health*, 30(1), e3.

---

# 17

---

## EVACUATION PLANNING AND PREPAREDNESS IN THE AFTERMATH OF KATRINA, RITA, IRENE, AND SANDY: LESSONS LEARNED\*

DAVID S. HELLER

*Regional and Systems Planning, South Jersey Transportation Planning Organization,  
Vineland, NJ, USA*

### 17.1 INTRODUCTION

In the midst of a natural disaster such as a hurricane, tornado, earthquake, or any other of a multitude of natural phenomena, the first thing on the mind of the affected citizenry is evacuation to a safer area. A smooth and efficient evacuation depends on many things, including the evacuation plans in place, the state of the transportation infrastructure, the command and control system in place, the strength and reliability of the communication system, and the availability and accessibility of shelter. Any chink in the multifaceted armor that comprises emergency evacuation can have severe consequences, ranging from loss of life to destruction of property and even anarchy. While probably the most vivid example of this breakdown in emergency

\*The contents of this report reflect the views of the author who is responsible for the facts and the accuracy of the data presented herein. The contents do not reflect the official views or policies of the South Jersey Transportation Planning Organization (SJTPO), its member jurisdictions, the SJTPO Policy Board, the South Jersey Transportation Authority (SJTA), or the FHWA. This report does not constitute a standard, specification, or regulation.

response was New Orleans and vicinity in the aftermath of Hurricane Katrina in August 2005, there have been numerous other examples, including Hurricane Rita in September 2005, Hurricane Irene in 2011, and, most recently, Hurricane Sandy in 2012. Using Hurricane Katrina as a focal point, this chapter describes and evaluates the evacuation plans and activities. The chapter concludes with methods and management schemes that will be used by emergency management coordinators and public officials to better prepare and mobilize communities against significant weather events such as these.

## 17.2 COMPONENTS OF A PREFERRED EVACUATION PLAN

Evacuation can be defined as the temporary but rapid removal of people from a building or disaster (or threatened) area as a rescue or precautionary measure (<http://www.business.dictionary.com/definition/evacuation.html>). It falls under the “response” phase of emergency management. An evacuation plan can be defined as a plan of action for citizens and emergency management officials to follow when faced with the necessity to evacuate due to an impending incident of natural or man-made disaster.

Even though an evacuation *plan* does not necessarily ensure a successful evacuation, there are certain common elements that all evacuation plans should contain. A successful evacuation has multiple phases, beginning with **planning and preparedness**, followed by **readiness**, and culminating with **activation**. The components of a successful plan are listed in Table 17.1.

Of course, any “preferred” plan can only exist on paper as every natural disaster is different. A strong hurricane plan can only do so much. For many of the reasons cited throughout this chapter, emergency response and evacuation planning is best done on a *regional* basis. Frank McCall, Cape May County (NJ) Emergency Management Director, has said that no municipality can respond on its own to a catastrophic event. Probably, the most important characteristic in any successful evacuation effort, however, is *flexibility*. The very unpredictable nature of natural disasters makes perfect planning almost impossible.

## 17.3 EVALUATION OF EMERGENCY PLANS AND ACTIVITIES

### 17.3.1 Katrina

Although evacuation plans existed at the federal, state, and local levels, ignorance of these plans, inadequate provisions within these plans, or even a failure to implement these provisions resulted in more severe consequences for the people the plans were designed to protect.

While the National Response Plan (NRP), the major federal plan in place, outlined a clear course of action in the event of a catastrophic emergency and/or disaster, as Hurricane Katrina was, it did not adequately provide a way for federal assets

**TABLE 17.1 The Components of a Successful Evacuation Plan****1. Planning and preparedness**

- Involve all agencies with evacuation responsibility in the development of the evacuation plan
- Identify the ultimate decision maker, as well as those with the authority and responsibility for issuing an evacuation order. Make sure their tasks are predefined
- Determine if the community needs additional training and resources to support an evacuation
- Inform community residents of the steps they should take to prepare for an evacuation, including whether they are located in an evacuation zone, what evacuation routes they should use, and the locations of nearby shelters
- Identify all available local resources
- Contain a strategy for special needs populations
- Identify decision points/triggers for the implementation of an evacuation order based on the catastrophic hazard
- Identify the estimated time needed to complete the evacuation, and coordinate with the appropriate highway, law enforcement, and transit agencies
- Provide for the timely communication of evacuation instructions to prepare people in advance of the order to evacuate
- Include provisions for communicating with people that have limited English proficiency
- Include provisions for evacuating transient populations (e.g., tourists, seasonal workers, and the homeless)
- Include the use of public transit vehicles, school buses, and paratransit vehicles

**2. Readiness**

- Identify the causes for an evacuation
- Include a mechanism for alerting key officials ahead of the need to evacuate
- Document the decision criteria to be monitored and evaluated before issuing an evacuation order
- Determine the size of the area to be evacuated and the number of people affected

**3. Activation**

- Identify the person who issues the evacuation order
- Describe how and when the evacuation order is communicated to the public
- Define the specific criteria for issuing a voluntary, recommended, or mandatory evacuation order
- Identify a system for notifying and coordinating with neighboring jurisdictions about what evacuation routes should be used and when

*Source:* FHWA (2007). “Components of an Effective Evacuation Plan.” Available at: [http://ops.fhwa.dot.gov/publications/evac\\_primer/19\\_components.htm](http://ops.fhwa.dot.gov/publications/evac_primer/19_components.htm)

to quickly supplement or supplant (if necessary) first responders. In its detailed analysis of the response to Hurricane Katrina entitled “A Failure of Initiative,” the US House of Representatives’ *Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina* found that federal agencies, including the US Department of Homeland Security (DHS), had varying degrees of unfamiliarity with their roles and responsibilities under the NRP (Heller 2010, US Congress House 2006).

Aside from the failure to implement the guidelines in the various evacuation plans that were in place at the time of Katrina, there were breakdowns in the actual

evacuation procedures following Katrina's landfall. For example, there were significant delays of government in issuing mandatory evacuation orders. High-level officials at all levels seemed to be ignorant of any formal evacuation procedure or what the plans stipulated. On Saturday, August 27, 2005, 2 days before Katrina made landfall just southeast of New Orleans, Michael D. Brown, director of FEMA, received a briefing from the National Hurricane Center on the severity of the hurricane and the likelihood that it would make a direct hit on New Orleans. Instead of acting quickly and dispatching emergency response management teams to the region, normally a reflex action of most FEMA directors, he just let the day pass. He sent two public affairs officials and waited to see what would happen. Senator Mark Pryor (D-Arkansas) would later testify to Congress that when FEMA finally did show up they really didn't have any real resources they could give (Heller 2010, p. 157).

There was also the delayed response by Mayor Ray Nagin. Though it was weak and somewhat vague, Mayor Nagin still didn't abide by the tenets of the New Orleans emergency management plan. The plan instructed that when a serious hurricane approached, the city should evacuate 27 h prior to the storm to give the "approximately 100,000 citizens of New Orleans [who] do not have the means of personal transportation" enough time to leave. In spite of this mandate, Mayor Nagin did not issue a mandatory evacuation order until the morning of Sunday, August 28, 19 h before the hurricane made landfall (Heller 2010, p. 158). Even though this was much later than what the plan called for, for some regions of the country, such as Cape May County, 19 h may be as "advanced" a warning they can expect.

In addition to the delay by all levels of government in issuing a mandatory evacuation order to the soon-to-be-displaced victims, there was a massive communications problem among multiple parties, which severely impaired the evacuation effort and *interoperability* between the different levels of government. More than 3 million customer telephone lines were knocked down in Louisiana, Mississippi, and Alabama; and as of September 28, 2005, almost 1 month after Katrina made landfall over New Orleans, over 238,000 customer lines in Louisiana alone still remained out of service. The wire line switching centers that route calls and the lines used to connect buildings and customers to the network also sustained significant damage. In addition, thirty-eight 911 call centers went down. It is clear that without a functioning, operable communications system in place, almost any evacuation effort is severely compromised.

In recent years, emergency planning and preparedness, especially on the government side, has been strengthened with the advent of the Internet and social media. In past years, it might have taken weeks following a major weather event to issue alerts, address issues or questions, and share information. Now, within minutes, or even seconds, state and local agencies can gather information and react appropriately, even in real time. What makes this possible is government's growing inclusion of social media applications in emergency operations, public safety, and homeland security operations. Governments are using the technology in a new paradigm of data exchange, not only broadcasting information to citizens, but gathering data from them and using it to drive decisions and services. While government has been slower than some entities to adopt these new technologies, Sandy showed this is

changing for the better. Agencies have an unprecedented opportunity to connect with communities on a whole new level, which is becoming more possible given the increasing portability and ease of using social media.

For a successful evacuation, there needs to be adequate and well-equipped shelter to house and support evacuees. The Louisiana Superdome, which housed as many as 30,000 evacuees at one time, was really deemed by Mayor Nagin as a “shelter of last resort.” It was also about 12 ft below sea level. Further, the Superdome was “not designed to be a long-term campground.” As the predominant shelter in the city, the Superdome was not enough (Heller 2010, p. 165).

While state plans such as the Southeast Louisiana Catastrophic Hurricane Plan (SLCHP) did exist, Louisiana as a state was relatively weak in its management capabilities. The power rested, predominantly, in the parishes. There existed very little communication between the state and its parish system.

Because of the weakness of the state, the federal coordinating officials met separately with each parish to provide recovery dollars and other resources (Heller 2010, p. 157). Even when plans did exist, the weak intergovernmental system of New Orleans’ emergency management system impinged on the successful implementation of both the SLCHP (described earlier) and the New Orleans comprehensive emergency management plan (described later).

As described earlier, even though the City of New Orleans did have an emergency management plan in place, it didn’t have any novel ideas or fresh approaches. For instance, the plan suggests that evacuation zones, based on “probable storm flooding,” should be used as the basis of mass evacuation. The plan further states that the evacuation zones are “pending further study.” But they never were fully developed (Heller 2010, p. 156). In summary, “the City of New Orleans followed virtually no aspect of its emergency management plan in the disaster caused by Hurricane Katrina...New Orleans also officially failed to implement most federal guidelines (Heller 2010, p. 156).” So, a failure to implement local plans was definitely a breakdown in the Katrina aftermath.

Though the failures greatly overshadowed the successes, there were a few bright spots in the evacuation following Hurricane Katrina. Data showed that more people were able to evacuate the city in a shorter time than originally people had thought. Traffic records analyzed after the evacuation showed that between 80 and 90% of all residents in the New Orleans area were able to evacuate, in about half of the 72 h clearance time that was originally estimated for that area (Wolshon 2006). Some of the preplanned operations strategies, such as contraflow, were implemented effectively, which further expedited vehicular evacuation. Unfortunately, for those 100,000–300,000 residents who could not or would not leave the city, the catastrophic impacts they endured greatly outweighed the positive result of a high evacuation participation rate.

### 17.3.2 Rita

Hurricane Rita followed on the heels of Hurricane Katrina, hitting the Louisiana and Texas coasts on September 24, 2005. In direct contrast to Hurricane Katrina, more residents than anticipated responded to evacuation instructions. (Of course, this

could also be due to the heightened awareness of Katrina, fresh on the minds of many Houstonians.) Hurricane Rita also slammed into an area that was wealthier, more mobile, and less densely populated than Katrina (O'Driscoll et al. 2005; USA Today 2005).

Following the ordeal, the Harris County (Houston) emergency management coordinator explained that their evacuation models envisioned 0.8–1.2 million people evacuated; but in reality, more than 2.5 million people fled Rita. This resulted in significant automobile traffic problems. Approximately 3 million people evacuated the Texas coast, creating 100 mile long traffic jams that left many stranded and out of fuel. Many fuel stations ran out of gasoline, because fuel truck drivers did not report to work. At a task force convened by the governor following Rita, Galveston City Manager Steve LeBlanc testified that the plan called for a sequenced evacuation, but “it just didn’t get followed (Litman 2006).” Like the Katrina evacuation, although not as widespread, a failure to follow through on existing emergency evacuation plans has definitely had some serious consequences for an area’s evacuees.

### 17.3.3 Irene

The challenges in successful hurricane evacuation planning are not unique to the New Orleans, Louisiana region. The State of New Jersey, with its 130 miles of Atlantic coastline, lies in an area very susceptible to hurricanes. Atlantic City has its own hurricane preparedness plan. Although residents know that it exists, tourists do not. Atlantic City has over 33 million visitors a year, which amount to approximately 275,000 persons a day (interview with Tom Foley, January 21, 2011). According to the Chief of Emergency Services for Atlantic City, the plan is effective, but it requires coordination and the participation of many government agencies with the casinos and other hotels.

There are some unique challenges to Atlantic City. Because of the city’s location on a barrier island with limited connections to the mainland, the City of Brigantine, which lies to the northeast of Atlantic City, has to evacuate before Atlantic City. Further, other cities depend on Atlantic City’s resources (e.g., buses) in their evacuation plans. Atlantic City’s buildings are also not hurricane proof. They were built to withstand a category 2 hurricane, which includes winds of up to 110 mph, while the parking garages are built to withstand even lesser winds of up to 75 mph.

As evidenced by Atlantic City’s evacuation procedures, coordination with other state and federal agencies is essential in any successful emergency evacuation drill. Effective emergency management depends on building relationships, sharing information, and coordinating plans, so that if a disaster takes place, the response will be as efficient and orderly as possible. The State of New Jersey has one of the best emergency operations procedures in the country because of the centralized command and control structure under the New Jersey State Police. Though New Jersey has 21 county emergency management coordinators and 567 city emergency management coordinators, the New Jersey State Police heads all emergency management activities in the state. If Atlantic City needs extra buses to facilitate its evacuation procedure, the State Police can order NJ Transit, the state’s chief transit agency, to donate buses. At the time of Hurricane Katrina, Louisiana did not have the same authority over its

emergency management resources that it could direct to the City of New Orleans (interview with Tom Foley, January 21, 2011). Overall, because of good emergency planning and evacuation plans in place, southern New Jersey experienced little in the way of casualties due to Hurricane Irene. Largely because of sufficient advance planning, and a much weaker storm than expected, there were no injuries or deaths in the evacuation of Cape May and Atlantic Counties and just seven New Jersey deaths in all. Many officials also believe that Governor Chris Christie's early and decisive actions contributed significantly to evacuation success. On August 25, 2011, a mandatory evacuation order was put into effect for Cape May County and the barrier islands. This was reinforced by an August 26 press conference televised statewide in which Christie warned viewers to "get the hell off the beach." However, evacuation activities were largely complete by 3:00 P.M., on August 27, more than 48 h before Irene made landfall as a tropical storm on the following day. Mandatory evacuation orders were issued for an estimated 1 million permanent and seasonal residents, resulting in an overall evacuation participation rate of 83% (Carnegie 2012).

Because of effective preplanning and proactive facility management, the evacuation of nursing homes and long-term care facilities went smoothly and according to facility plans. Further, pet evacuation and sheltering operations were deemed successful (Carnegie 2012). However, the evacuation of the most impacted areas in southern New Jersey certainly wasn't flawless. In a post-Irene emergency preparedness conference, emergency management officials cited a lack of adequate shelter as a problem. Since 1992, Cape May County has not had any shelters that can withstand a category 1 or greater hurricane. This is mainly because more than 80% of the population would be severely impacted, if not underwater, and county officials do not want anyone to stay there (interview with Francis J. McCall, August 15, 2011). In addition, they need to be better equipped, especially for prolonged periods of displacement. Residents should know where their shelters are, in addition to having their own emergency preparedness kits with potable water, flashlights, batteries, and nonperishable goods. Shelters set up around the state were not prepared for the extended power outages that could have occurred if Hurricane Irene had the impact that was originally predicted (Degener 2011). The storm hit on Saturday, August 27, 2011, and most residents returned to their home on the next day, Sunday night. If Irene was stronger or longer, then more food, cots, and other supplies would have been needed (Degener 2011).

The transportation for those who lacked their own private vehicles could also have been better planned. Even though 98% of its people were evacuated, the buses used to transport evacuees out of Atlantic City in advance of Hurricane Irene were not deployed as efficiently as they could have been. The private bus companies that supplied buses to Atlantic City for the evacuation effort were supposed to be used as shuttles to nearby points, from where they would then be taken to other shelters further north by NJ Transit buses (Lemongello 2011). But, because NJ Transit was already "taxed to the limit" in accommodating their regularly scheduled service, these shuttles ended up taking people directly to shelters as far as Warren and Mercer counties, more than 100 and 150 miles, respectively, away from Atlantic City (Lemongello 2011).

### 17.3.4 Sandy

In what would become known as the worst storm to hit New Jersey, Hurricane Sandy made landfall near Atlantic City on October 29, 2012. Sandy destroyed more than 72,000 homes in New Jersey and knocked out power to more than 8.5 million homes to people in 16 states as well as the District of Columbia. Sandy also claimed the lives of 123 people (UPI.com 2012). Sandy is estimated to have caused \$62 billion in damages, mostly in New York and New Jersey, making it the second costliest storm on record after Katrina (Huffington Post 2012b).

Since Sandy was a rather unusual storm, in that it was a combination of a hurricane with a nor'easter, and it had incredible power, even a more extensive evacuation effort than was already ordered would most likely not have mitigated the damage. More than 24 h before Sandy made landfall, Governor Christie declared a state of emergency and ordered a mandatory evacuation for all the barrier islands from Sandy Hook to Cape May. He also said that people should be prepared for power outages lasting up to 10 days (CBS2 New York 2012). His warnings were reinforced by numerous media outlets and Internet websites. Nevertheless, more mandatory evacuation orders for some areas could probably have helped, as residents in some cities that suffered extensive flooding found themselves trapped in their apartments and houses. In Hoboken, NJ, one resident who was trapped in her apartment for more than 2 days in fetid conditions said she wishes that the city had issued mandatory evacuations for all residents in flood-prone areas, as opposed to just those in ground-floor units (Huffington Post 2012a). While adequate evacuations and procedures may not have been perfectly enforced for every jurisdiction, it appears that emergency preparedness and planning for Sandy has come a long way from the relative chaos and anarchy that followed Katrina.

While this concludes the section on critical breakdowns in the posthurricane evacuation processes, this certainly does not represent an exhaustive list of all the major reasons for unsuccessful hurricane evacuations. There are other reasons for the poor evacuation and recovery effort in Katrina's (and other hurricanes') aftermath. Some people refuse to leave, feeling an emotional attachment to their home or feeling they have nowhere else to go. Shortly after Irene, a poll on social networking sites questioned people if they would evacuate again given what happened in Irene. Some respondents stated they may not want to leave next time, especially since Irene wasn't as destructive to Cape May County as predicted. Another explanation behind this response is that some evacuees found conditions worse where they relocated (Fichter 2011).

In 2007, the Harvard School of Public Health conducted a poll on the top reasons people refuse to evacuate in a hurricane (Harvard School of Public Health 2007a). The reasons and associated percentages are as follows:

- They think home is well built/will be safe (75%).
- They think the roads will be too crowded (56%).
- They think evacuation will be too dangerous (36%).
- They are worried that possessions would be stolen or damaged (33%).
- They do not want to leave pet (27%) (Harvard School of Public Health 2007b).

Finally, another reason evacuation planning could fail is simply due to the destructive and unpredictable nature of the storm, as was the case in Hurricane Sandy. Who could have predicted the extent of destruction that Sandy wrought, especially since most people in the affected areas hadn't experienced anything like it in more than 30 years?

#### **17.4 SUGGESTIONS ON IMPROVEMENTS, NEW METHODS, AND MANAGEMENT SCHEMES**

Given the caveat that even the most comprehensive emergency evacuation plans cannot ensure or guarantee a smooth or flawless evacuation, there are certain deficiencies found in many existing evacuation plans that, if remedied now, can help increase the odds of attaining a flawless evacuation.

- **Stronger Interaction between Emergency Officials and Transportation Officials**

As evidenced by many of the large-scale evacuations instigated by hurricanes, emergency preparedness cannot be separated from other aspects of transportation systems and infrastructure. Emergency planning is inextricably linked to overall good transportation planning, and it is not possible to have poorly maintained roads and expect emergency response activities to function smoothly in a crisis. There must be constant interaction between emergency officials and other transportation officials to ensure that crisis response is incorporated into a community's overall transportation plan. Public officials must think of evacuation as a systemic challenge tied to large-scale transportation and economic patterns, rather than as simply a crisis-time response activity (Kendra et al. 2008).

- **More Attention and Resources Devoted to Preparedness**

Just as Louisiana had its Hurricane Pam simulation exercise a little more than a year prior to the onslaught of Katrina, there needs to be many more of these "preparedness" exercises taking place. In July 2011, the Cape May County Office of Emergency Management convened the "Escape the Cape 2011" emergency management exercise at an area high school. The purpose of the exercise was to evaluate interagency and intergovernmental coordination at the municipal, county, state, and federal levels using the National Incident Management System (NIMS) in preparation for, response to, and recovery from a hurricane. More than 210 people participated in the 2-day exercise that also included 13 federal partners and 23 state partners (Herald Staff 2011). Usually, state and federal agencies coordinate these regional drills. But, this time, they were partners, with the *county* being the lead agency (interview with Francis J. McCall, August 15, 2011). The county pushed for this, in part, because of the lackluster federal response to Hurricane Katrina.

In Hurricane Katrina, Mayor Nagin gave residents the order to evacuate 19 h prior to the hurricane making landfall. This was much shorter than the 72 h time

span recommended by the New Orleans plan, which is similar to the Cape May plan. The “Escape the Cape” exercise seems to have paid off for the county, as just about a month later, when Hurricane Irene hit the New Jersey coastline, almost 800,000 people were successfully evacuated without incident (Degener 2011). The alert was issued August 25, 2011, at 2:00 P.M., almost 72 h before Irene made landfall on August 28, 2011 at 5:35 A.M. (AccuWeather.com 2012; CapeMay.com 2012).

Preparedness is a key component in the Atlantic City’s emergency response procedures. Tabletop drills are conducted at one of the numerous events hosted by Atlantic City every year (interview with Tom Foley, January 21, 2011). A tabletop exercise is a simulated scenario designed to test the response capability of an organization to a given event. The scenario(s) requires a coordinated response to a realistic situation that develops in real time with participants gathered to formulate responses to each development (<http://www.innovateonline.info/extra/definition3492.htm>). For the annual Atlantic City air show that attracted up to 800,000 people in August 2011, the emergency response team practices evacuation procedures, including interoperability, communications, emergency management services (EMS), and fire rescue (interview with Tom Foley, January 21, 2011).

The emergency management office for Cape May County has actually made a recommendation to the state that a hurricane’s prelandfall declaration be an emergency declaration. Prior to Hurricane Katrina, neither FEMA nor the State of New Jersey did not consider any sort of prelandfall event or declaration to be an emergency (interview with Francis J. McCall, August 15, 2011).

- **Greater Incorporation of Modern Technology in Disaster Management and Response**

Concomitant with increased preparedness is the incorporation of modern technology, including faster telecommunications links and the use of social media, which can strengthen disaster management and response. Nowhere was this more evident than in the response to Hurricane Sandy. With widespread followers and usage, social media applications such as Facebook can serve to quickly mobilize volunteers in emergency response and recovery. Largely due to a widely seen and followed Facebook page as well as numerous Twitter hashtags, “Rebuild Staten Island” was able to convene enough volunteers to clean 140 houses in the Tottenville neighborhood of Staten Island in just the first day of volunteering alone. Occupy Sandy, a spin-off of the widespread and heavily publicized Occupy Wall Street, has been able to sign on more than 15,000 volunteers, all through the Web, and was serving 10,000 meals in the Sunset Park neighborhood of Brooklyn in the first week after Sandy (SIIlive.com 2012).

The federal government is also making more extensive use of social media in its emergency response and recovery operations. FEMA uses social media to crowdsource information. Further, the agency actively monitored Twitter during Hurricane Sandy for incidents and situational awareness, for example, what

areas were flooding. Agencies such as the Red Cross also monitored Twitter for Sandy-related posts (of which there were approximately 2.5 million) and followed up on more than 4500 of them (SIIlive.com 2012). Start-up companies that aid in disaster recovery utilizing social media have emerged. One such example is recovers.org, a small start-up operating out of Massachusetts that has developed a tool easily retrievable by communities that can allow them to post updates on storm recovery operations, as well as to enlist volunteers (SIIlive.com 2012).

Social media possesses other advantages in disaster recovery. Social media often beats traditional media in reporting a crisis. For example, the primary source of information for the 2010 Haiti earthquake was not the television news media, but Twitter. Social media networks are also dynamic; the content can be continually updated to present real-time information to the users. Further, many social media applications now have a geotagging feature, which could allow first responders to pinpoint with some precision where someone in danger or needs help is located (Gilmore and Social Media Blog 2010). For these reasons and more, the role of social media in disaster preparedness and recovery is only going to continue to increase, as the technology improves and devices transmitting social media become more prevalent and economical for everyone to acquire.

- **More Attention to Special Needs Population**

As noted previously, a successful evacuation plan needs to contain provisions for the evacuation of that segment of the population with special needs—particularly, those who have a mobility impairment, such as the poor, the disabled, and the elderly. One strategy that has been implemented in Cape May County as a direct consequence of Hurricane Katrina (where some nursing homes were abandoned causing the deaths of 100 people) is a plan for evacuating the residents of nursing homes. The county has been working with the nursing homes for the past several years in writing evacuation plans, making sure that the appropriate transportation resources are lined up and alternate facilities are identified where residents can be relocated.

- **Overcoming Resistance to Evacuation**

As seen in Hurricane Katrina and depicted in Table 17.1, many people in the midst of a hurricane evacuation refuse to leave. These include lower-income people who lack a vehicle and money, people who have no place to go and are fearful of conditions in emergency shelters, people who want to protect their homes and/or pets, and many “hearty” souls who just feel that they can ride out the storm. While attaining a 100% evacuation rate may be impossible, various strategies can be used to increase evacuation rates. These include providing more information on the risks facing people who stay, subsidized transportation, more comfortable and secure shelters, and better protection of homes. Although providing subsidized transportation may incur a slight cost at the outset, it would be quite small compared to the costs in terms of lives lost that could be avoided (Litman 2006, p. 11). Provisions should also be made well beforehand for pets, as Atlantic City has already done with ensuring an animal

shelter at the Atlantic City Race Track. Since the most common reason for residents' refusal to evacuate is a belief in the safety of their own home, as indicated in Table 17.1, then perhaps emergency management officials in charge of storm preparedness should place the most emphasis on educating their citizens on storm-resilient housing materials and how their own dwelling unit measures up. The dissemination of graphic pictures, such as those depicting extensive damage due to Sandy, might serve as a good vehicle to educate citizens and prod them into compliance with hurricane evacuation orders.

- **Planning for Resilience**

*Resilience* refers to a system's ability to accommodate variable and unexpected conditions without catastrophic failure or "the capacity to absorb shocks gracefully (Litman 2006, p. 13)." Any successful evacuation effort requires both a well-maintained and resilient infrastructure system. Resilience can increase if a system has effective ways to prioritize resources. For example, buses and trains should be given priority in an evacuation where needed to avoid congestion and bottlenecks or to use limited fuel resources more efficiently. The design of "failsafe" components of the transportation system can enhance a transportation system's resilience. For example, where possible, roundabouts should be used in place of traffic signals, as they can function without electricity. The implementation of a contraflow lane(s) to increase evacuation capacity, as described earlier, also enhances a system's resilience. In an evaluation of Cape May County's Hurricane Irene evacuation, the New Jersey State Police Office of Emergency Management noted that the increased number of lanes due to the implementation of the reverse-lane strategy on major county highways leading traffic out nearly halved evacuation times from the shore (Degener 2011).

An effective plan for debris removal can also enhance a system's resilience and expedite recovery. In the aftermath of Irene and especially Sandy, many towns were not prepared for the amount of debris the storm created. Debris removal plans that outline manpower and equipment need to be in place. Recovery activities following a disaster must start with clearing roads of trees and downed power lines (Degener 2011).

Coordination with transportation agencies such as the South Jersey Transportation Planning Organization (SJTPO) and the New Jersey Department of Transportation on specific transportation improvements can effectuate a successful evacuation. For example, the Garden State Parkway and the Atlantic City Expressway, two major evacuation routes in the southern New Jersey region, are in the process of being expanded. Bridges and causeways that provide access to and from the shore towns also need to be raised. In these fiscally constrained times, these projects may not be easily budgeted. The policies and design concepts described here constitute just a few of numerous strategies to increase a system's resilience.

- **Restrict Development in Vulnerable Areas**

Hurricane Sandy has reignited the debate for allowing development in vulnerable areas, such as coastlines. Even though there have long been strict building codes

and man-made storm barriers such as seawalls and dunes constructed in many coastal areas, many officials wonder if we should be building anything in these areas at all, especially in light of continuing sea level rise. One option that has been floated by many is for the federal government to buy property in flood-prone areas to prevent development at all. Since 1989, FEMA has spent close to \$10 billion to purchase homes in vulnerable areas and relocate them (Osborne 2012). However, with the federal government on the verge of a fiscal cliff and facing a debt of more than \$16 trillion and counting, this doesn't figure to be a viable alternative, at least in the near term. Further, some coastal states, such as New Jersey, have lax development regulations. While owners of coastal developments in New Jersey can rebuild in the wake of storms, other states, such as North Carolina, do not allow rebuilding in the same place after a home or business is damaged by a hurricane. They require property owners to comply with new setbacks from the beaches, which have proven to be effective in minimizing storm and flood damage (Osborne 2012). In any case, more stringent regulation of development along coastal areas is practically a must in mitigating impacts from a hurricane.

- **Greater Involvement from the Private Sector**

As intimated previously, governments frequently operate within very tight budgets and limited resources, which may constrain their ability to do successful emergency and evacuation planning. As has been shown in this chapter, no single entity has the wherewithal to sustain itself independently in a major incident such as a hurricane, especially in a state as parochial as New Jersey. One of the major industries in South Jersey is tourism. If visitors and tourists cannot evacuate in a major incident or feel unsafe in any way, everyone will suffer. As such, those businesses that depend on tourism need to be more involved in emergency prevention and preparedness. The City of Atlantic City works extensively with the casino operators in developing its hurricane preparedness plan. Casinos are also members of Atlantic City's Local Emergency Planning Committee (LEPC), which are public-private partnerships mandated by the Superfund Amendments and Reauthorization Act (SARA) Title III Act in communities where hazardous materials are present. Since this act was first promulgated, LEPCs have expanded their mission to include natural, technological, and civil disasters—the all-hazards approach to emergency planning (NJ Office of Emergency Management 2011).

Greater involvement from the private sector can also come in the form of monetary contributions to agencies that provide emergency relief services, such as the Red Cross. The Red Cross Annual Disaster Giving Program (ADGP) supports Red Cross disaster efforts by pledging donations to the Red Cross in advance of major disasters to ensure an immediate response to those that are affected. The ADGP members consist of numerous Fortune 500 corporations, including FedEx, Lowe's, UPS, and Walmart (American Red Cross 2011, 2012). Other large corporations, such as General Electric and Home Depot, have foundations that provide an abundance of resources in terms of both manpower and money to communities that have been ravaged by natural disasters.

Indeed, for many of these corporations, disaster preparedness and recovery has become a major part of their operations and, often times, serve this function more effectively than the federal government. Since Katrina, the federal government has been studying ways to improve emergency response by working with the private sector. During Hurricane Katrina, Walmart was able to open its stores in the New Orleans area within a week after the levees broke and deliver \$20 million in cash, 100 truckloads of free merchandise, and food for up to 100,000 meals. Walmart also has a staff meteorologist that keeps track of disasters and ensures timely responses. They utilize an extensive database to help anticipate demand and ensure that their stores are stocked up with needed products (TriplePundit 2012). Public agencies have taken notice, as the State of Florida's Division of Emergency Management is headed by Brian Koon, who was formerly Walmart's emergency response manager (NPR 2012).

Home Depot, another Fortune 500 corporation, has an active hurricane command center staffed by more than 100 associates during hurricane season who work with district managers who, in turn, work with store managers to ensure that their stores are adequately equipped with storm recovery materials such as generators, chain saws, and water. In addition, many of Home Depots' stores are backed up by emergency generators, as was demonstrated by their immediate reopening in Puerto Rico, 1 day after the Irene struck (NPR 2012). In his paper, "Wal-Mart to the Rescue: Private Enterprise's Response to Katrina," Professor Steven Horwitz argues that Walmart's successful response to Katrina victims, especially in comparison to FEMA and other government agencies, seem to confirm the conclusion of modern political economy that private sector corporations are better at mobilizing resources in ways citizens want than public agencies (Horwitz 2008). The successful emergency response efforts by both Home Depot and Walmart, two of the largest retail operations in the country, have demonstrated that the private sector should continue to play an integral role in disaster management and recovery operations.

The private sector should also be involved in the procurement of vehicles, that is, buses, trucks, and vans, that will be needed to quickly transport people and supplies out of and into the evacuation area. Good preparedness should also involve the preparation of standby emergency service contracts with private transportation providers to fill transit service gaps (should any arise) and to help provide for refueling of vehicles away from transit facilities. Needless to say, these contractual arrangements, including indemnification and funding agreements, should be worked out well in advance of the actual incident (TRB Special Report 2008). As described earlier, in the case of Hurricane Katrina, if the "contractual requirements" with the bus companies had been worked out in advance of the storm, the idle buses could have been utilized and more lives might have been saved. Recognizing that transit agencies typically don't have emergency response as their primary mission, and local emergency response plans tend to be more locally oriented while disasters span multiple jurisdictions, state governments should take the lead in developing these regional evacuation

plans, coordinating with the appropriate regional entities as appropriate (TRB Special Report 2008, p. 9).

Because businesses are profit driven, as opposed to public sector entities, which are driven by other goals, incentives to solicit their involvement in emergency management may be needed, particularly in the case of smaller businesses that lack the resources of Walmart or Home Depot. The private sector can be reluctant to participate in the disaster management effort if they feel they are carrying most of the financial burden. In this vein, the public sector could craft legislation to limit liability in any disaster preparedness or response effort and incentivize insurance companies to underwrite contingency planning and resilience building (National Academy of Sciences 2010). Another added benefit for the private sector to engage in resilience building would be to increase the purchasing power of their customers and minimize the time needed for economic recovery. Organizations that set up disaster contingency and business continuity plans are likely to be more resilient in the event of a disaster, giving them an edge over their competitors (National Academy of Sciences 2010).

In addition to helping out directly in the disaster preparedness and recovery efforts, the private sector can assist in the financing of storm repair and recovery efforts typically much faster than the federal government can via the National Flood Insurance Program (NFIP) or any other public insurance program. To this end, some governments have purchased a parametric insurance policy as an alternative to a traditional insurance policy. In addition to the speed at which payment under this type of insurance is processed (typically 2–6 weeks, as opposed to traditional insurance that could be months or even years), another advantage of this type of policy is that the proceeds can be used at the buyer's discretion, whereas under a typical insurance policy, the payment is intended to cover just the loss that was sustained. Under a parametric policy, payments are usually triggered by an event with some measurable parameter—for example, a hurricane of 960 mb or lower or an earthquake measuring 5.0 on the Richter scale. Once the event happens, no further adjustment is needed (Linkin 2012). The State of Alabama, in addition to other public entities, has purchased this type of insurance policy to pay for increased insurance costs following a hurricane (Linkin 2012).

## 17.5 CONCLUSION

As long as there are cities and population growth along the coastlines, hurricanes and the subsequent need to evacuate will be a constant risk. While hurricanes themselves cannot be avoided, man's vulnerability to their effects can be reduced through effective planning and preparedness (Wolshon et al. 2001, p. 5) However, in order to effectuate a smooth evacuation effort, there needs to be a solid bureaucratic as well as physical infrastructure in place. As was seen throughout this chapter, effective emergency planning and response requires extensive interagency coordination and collaboration, involving a multitude of professional talents. Effective evacuation

planning is also a regional concept, requiring the collaboration of multiple jurisdictions, as a natural incident such as a hurricane knows no political bounds. The devastating aftermath of Hurricanes Katrina and Sandy have served as a wake-up call to all Americans, in prompting a greater awareness and need for stronger emergency preparedness and response. Though the damage in terms of human life incurred by Hurricanes Sandy and Irene were much less than Katrina, there are still lessons to be learned from that evacuation effort that could increase preparedness and further lessen a hurricane's impact. Though some of the lessons learned from Katrina have been put into place, as evidenced by New Jersey's largely successful Irene evacuation, Hurricane Sandy unveiled a whole litany of additional challenges to emergency managers everywhere, in not just ensuring a successful evacuation of citizens with adequate shelters and provisions for mass care, but a reexamination of building and development decisions in vulnerable areas that put lives and property at risk. While advances in technology and social media have provided emergency managers with an array of powerful tools that can enhance emergency preparedness and response, it will take a continued collaborative effort between government at all levels, the private sector, and the public to ensure a truly resilient evacuation management system.

## REFERENCES

- AccuWeather.com. 2012. "Irene Makes Landfall in New Jersey, Approaching NYC." Available at: <http://www.accuweather.com/en/weather-news/mean-irene-closes-in-on-nc-out-1/54295>. Accessed December 29, 2012.
- American Red Cross. 2011. "Annual Disaster Giving Program." Available at: <http://www.redcross.org/supporters/corporate-foundations/annual-disaster-giving-program>. Accessed July 30, 2011.
- American Red Cross. 2012. "Red Cross Opening Shelters, Mobilizing Equipment as Hurricane Irene Heads Toward East Coast." Available at: <http://www.redcross.org/news/press-release/Red-Cross-Opening-Shelters-Mobilizing-Equipment>. Accessed June 15, 2012.
- CapeMay.com. 2012. "Mandatory Cape May County Evacuation for Hurricane Irene." Available at: <http://capemay.com/magazine/2011/08/hurricane-irene/#axzz2GBzAgk8G>. Accessed December 29, 2012.
- Carnegie, Jon. 2012. *Hurricane Irene Response: A Behind the Scenes Look at New Jersey's First Large-Scale Evacuation in Modern History*. National Evacuation Conference, New Orleans, LA, February 8–9, 2012. Alan M. Voorhees Transportation Center, Rutgers, The State University of New Jersey.
- CBS2 New York. "Christie Declares State of Emergency; Orders Evacuations in Some Parts of N.J." Available at: <http://newyork.cbslocal.com/2012/10/27/evacuations-begin-in-some-areas-of-new-jersey-for-hurricane-sandy/>. Accessed December 28, 2012.
- Degener, Richard. 2011. "Cape May County evaluates its own performance in Hurricane Irene evacuation." *The Press of Atlantic City*. September 20, 2011.
- FHWA. 2007. Components of an Effective Evacuation Plan. Available at: [http://ops.fhwa.dot.gov/publications/evac\\_primer/19\\_components.htm](http://ops.fhwa.dot.gov/publications/evac_primer/19_components.htm). Accessed January 30, 2011.
- Fichter, Jack. 2011. "Hurricane Experts: 'We Got Lucky with Irene'." *The Cape May County Herald*. September 21, 2011, Available at: <http://www.capemaycountyherald.com/article/>

- government/court+house/76378-hurricane+experts+039we+got+lucky+irene039. Accessed November 2, 2011.
- Gilmore, Glen and Social Media Blog. 2010. "10 Reasons Social Media Is Important in a Real Crisis." May 2010. Available at: <http://socialmediavoice.com/2010/05/10-reasons-why-social-media-is.html>. Accessed December 29, 2012.
- Harvard School of Public Health. 2007a. Project on the Public and Biological Security. Available at: <http://archive.sph.harvard.edu/press-releases/2007-releases/press07242007.html>. Accessed December 29, 2012.
- Harvard School of Public Health. Working Paper: High-Risk Area Hurricane Survey. Project on the Public and Biological Security. 2007b. Available at: <http://www.hsph.harvard.edu/horp/project-on-the-public-and-biosecurity/>. Accessed December 15, 2014.
- Heller, David S. 2010. "Evacuation Planning in the Aftermath of Katrina: Lessons Learned." *Risk, Hazards & Crisis in Public Policy*: Vol. 1: Iss. 2, 131–174, Article 5.
- Herald Staff. "Drill Tests 'Escape the Cape' as Mock Hurricane Jessica Barrels North." Cape May County Herald. July 28, 2011. Available at: <http://www.capemaycountyclerald.com/article/government/court+house/74869-drill+tests+039escape+cape039+mock+hurricane+jessica+barrels+north>. Accessed July 30, 2011.
- Horwitz, Steven. 2008. "Wal-Mart to the Rescue: Private Enterprise's Response to Hurricane Katrina." Version 2.0. June 2008. Available at: [http://myslu.stlawu.edu/~shorwitz/Papers/Wal-Mart\\_to\\_the\\_Rescue.pdf](http://myslu.stlawu.edu/~shorwitz/Papers/Wal-Mart_to_the_Rescue.pdf). Accessed December 29, 2012.
- Huffington Post. 2012a. "Sandy-Weary Hoboken Residents Criticize City over Evacuation Warnings." Available at: [http://www.huffingtonpost.com/2012/10/31/sandy-hoboken-evacuation\\_n\\_2052831.html](http://www.huffingtonpost.com/2012/10/31/sandy-hoboken-evacuation_n_2052831.html). Accessed December 28, 2012.
- Huffington Post. 2012b. "Superstorm Sandy Deaths, Damage and Magnitude: What We Know One Month Later." Available at: [http://www.huffingtonpost.com/2012/11/29/superstorm-hurricane-sandy-deaths-2012\\_n\\_2209217.html](http://www.huffingtonpost.com/2012/11/29/superstorm-hurricane-sandy-deaths-2012_n_2209217.html). Accessed December 28, 2012.
- Kendra, James, Jack Rozdilsky, David A. McEntire. (2008). Evacuating Large Urban Areas: Challenges for Emergency Management Policies and Concepts. *Journal of Homeland Security and Emergency Management*. Vol. 5, Iss. 1, 15–16, Article 32.
- Lemongello Steven. "Emergency Management Officials give Passing Grade to Hurricane Irene Evacuation." *The Press of Atlantic City*. August 29, 2011.
- Linkin, Megan. 2012. "Revive, Rebuild, Recover: Creating a Sustainable New Jersey Coastline." Presentation at Rebuilding a Resilient New Jersey Shore Conference," West Long Branch, NJ, December 7, 2012.
- Litman, Todd. 2006. Lessons from Katrina and Rita: What Major Disasters Can Teach Transportation Planners. Victoria Transport Policy Institute. Available at: <http://www.vtpi.org/katrina.pdf>. Accessed January 31, 2011.
- National Academy of Sciences. 2010. *Private–Public to Enhance Community Disaster Resilience: A Workshop Report*. Washington, DC: National Academies Press, p. 34.
- NJ Office of Emergency Management. 2011. "LEPC's Enhance Local Disaster Plans, Resources." Available at: [http://www.nj.gov/njoem/preparedness\\_lepcart.html](http://www.nj.gov/njoem/preparedness_lepcart.html). Accessed July 30, 2011.
- NPR. 2012. "Big-Box Stores' Hurricane Prep Starts Early." Available at: <http://www.npr.org/2011/08/26/139941596/big-box-stores-hurricane-prep-starts-early>. Accessed December 29, 2012.

- O'Driscoll, Patrick, Wolf, Richard, and Hampson, Rick. 2005. "Evacuation Worked, but Created a Highway Horror." *USA Today*. September 26, 2005. Available at: [http://www.usatoday.com/news/nation/2005-09-25-evacuation-cover\\_x.htm](http://www.usatoday.com/news/nation/2005-09-25-evacuation-cover_x.htm). Accessed June 17, 2012.
- Osborne, James. 2012. "Building Debate Along the Shore." *The Philadelphia Inquirer*. November 25, 2012, B1-B2.
- SIlive.com. 2012. "Social media aids Hurricane Sandy cleanup on Staten Island." Available at: [http://www.silive.com/news/index.ssf/2012/11/social\\_media\\_aids\\_hurricane\\_sa.html](http://www.silive.com/news/index.ssf/2012/11/social_media_aids_hurricane_sa.html). Accessed December 29, 2012.
- Transportation Research Board (TRB) Special Report 294. 2008. "*The Role of Transit in Emergency Evacuation*." Washington, DC: TRB, p. 126.
- TriplePundit. 2012. "Major Retailers Show that Disaster Management is an Integral Part of CSR." Available at: <http://www.triplepundit.com/2011/08/major-retailers-show-disaster-management-integral-part-csr/>. Accessed December 29, 2012.
- U.S. Congress House. 2006. A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. Available at: [http://katrina.house.gov/full\\_katrina\\_report.htm](http://katrina.house.gov/full_katrina_report.htm). Accessed November 10, 2010.
- UPI.com. 2012. "Superstorm Sandy Devastates New York, New Jersey." Available at: [http://www.upi.com/Top\\_News/US/2012/12/25/The-Year-in-Review-2012-Superstorm-Sandy-devastates-New-York-New-Jersey/UPI-74491356427800/](http://www.upi.com/Top_News/US/2012/12/25/The-Year-in-Review-2012-Superstorm-Sandy-devastates-New-York-New-Jersey/UPI-74491356427800/). Accessed December 27, 2012.
- USA Today. "Evacuation Worked, but Created a Highway Horror." September 26, 2005. Available at: [http://www.usatoday.com/news/nation/2005-09-25-evacuation-cover\\_x.htm](http://www.usatoday.com/news/nation/2005-09-25-evacuation-cover_x.htm). Accessed May 31, 2011.
- Wolshon, Brian. "Evacuation Planning and Engineering for Hurricane Katrina." *The Bridge* (2006): 32, 27-34. Available at: <http://www.nae.edu/File.aspx?id=7393>. Accessed May 31, 2011.
- Wolshon, Brian, Elba Alicia Urbina, Marc Levitan, et al. (2001). *National Review of Hurricane Evacuation Plans and Policies*. Baton Rouge, LA: Louisiana State University (LSU) Hurricane Center, p. 13.

---

# 18

---

## RURAL EVACUATION AND PUBLIC TRANSPORTATION

JAYDEEP CHAUDHARI<sup>1</sup>, ZHIRUI YE<sup>2</sup>, AND DHRUMIL PATEL<sup>3</sup>

<sup>1</sup>*Western Transportation Institute, Montana State University, Bozeman, MT, USA*

<sup>2</sup>*School of Transportation, Southeast University, Nanjing, China*

<sup>3</sup>*College of Education and Human Sciences, University of North Alabama, Florence, AL, USA*

### 18.1 INTRODUCTION

Small and rural communities around coastal areas, nuclear power plants, forests, or earthquake-prone zones are under frequent threats of hurricane, flood, nuclear fusion, earthquake, wildfire, and heavy rainfall. During natural disasters such as the devastating Hurricanes Sandy in 2012, Irene in 2011, and Katrina and Rita in 2005, people in coastal communities required mass evacuation and other major emergency transportation services. While planning and coordination among emergency management, law enforcement, and transportation agencies led to an effective system allowing anyone with a car to evacuate from urban areas, however, many vulnerable and public transportation-dependent rural residents were literally left behind during the hurricane seasons of the last 8–10 years. When evacuation takes place, rural coastal communities are at high risk and are difficult to evacuate in a timely manner due to larger geographical areas, low population densities, and limited resources such as alternate modes of transportation, food, fuel, lodging, and medical facilities.

Before 2005, public transportation operators in the United States did not take the lead on evacuation planning, nor were they viewed as a viable option for evacuation. There is an increased national awareness and interest in the role of public transportation in evacuation. Typically, emergency management agencies (EMAs) such as

police, fire, and emergency medical services—the first responders to an incident—take the lead in an evacuation. However, public transportation can perform multiple roles in evacuation and can be a successful partner in the four tasks of emergency management planning: (i) mitigation, (ii) preparedness, (iii) response, and (iv) recovery. For example, transit can provide evacuation for vulnerable, transit-dependent populations. Transit drivers can transport emergency personnel and equipment to an incident site. During reentry, after the emergency has passed, transit providers can move transportation-dependent evacuees to their original locations or other destinations, help supply real-time information on the extent of damage, and assist in efforts to resume normal service as quickly as possible.

The 2006 Nationwide Plan Review published by the Department of Homeland Security, in cooperation with the US Department of Transportation, indicated that very few states or large urban areas have adequately planned for evacuating people who are dependent on public transportation (Committee on Nationwide Plan Review Phase 2, 2006). This report also noted that most evacuation planning efforts focused on evacuation by personal vehicle with very little attention given to the role of public transportation systems. As compared to urban areas, rural areas are underserved by public transportation. However, school bus systems can serve as a substitute for public transportation in emergency events as they are widely available in rural areas throughout the nation. In fact, sometimes school bus systems are the only means of public transportation in rural areas. Information related to transit use in evacuations and emergency events is widely available for urban areas, but there is limited knowledge on rural public transportation. Nearly 40% of the country's transit-dependent population—primarily senior citizens, persons with disabilities, and low-income individuals—live in rural areas. Public transportation in rural areas is expected to play a greater role than envisioned for routine and emergency events.

Emergency management is a complex and multiagency emergency operation. If a public transportation system is not a part of a local emergency management plan, operations to evacuate transit-dependent populations can be jeopardized. This chapter focuses on what role public transportation systems can play, how adequately transit systems are prepared, and what challenges and issues may arise in the event of an emergency/evacuation. These questions are answered through a literature review, a survey, and the rural evacuation operations. The survey results are incorporated in the literature review and other discussions throughout the chapter. The case studies include three evacuation events: (i) the 1997 flood, the second largest evacuation in US history; (ii) the 2007 emergency response exercise that simulated a flood disaster in the Sacramento region; and (iii) Hurricane Sandy coastal counties evacuation.

## 18.2 LITERATURE REVIEW

A considerable body of literature exists on the role of transit in emergency evacuations. The literature has become extensive since the 9/11 terrorist attacks on the World Trade Center and Hurricane Katrina. In fact, a transit system played an

important role in evacuating people from the World Trade Center area following the September 11 attacks. These two events became the impetus for investigating the role of transit in evacuation and emergency events.

This literature review focused on the following topics:

- Public transportation systems in rural areas
- The role of public transportation in evacuation
- Public transportation systems in evacuation operations
- Evacuation practices in rural areas
- Actions implemented for emergency evacuation of rural areas

### **18.2.1 Public Transportation Systems in Rural Areas**

Public transportation includes a regularly scheduled transit system, demand-response transit for the elderly and disabled, intercity bus services, and car- and vanpooling. In rural communities, public transportation is provided by a variety of private sector, not-for-profit organizations, and various public agencies. Nearly 40% of the nation's transit-dependent residents live in rural areas, almost 38% do not have access to public transportation, and less than 10% of federal spending for public transportation is for rural communities. Today, there are approximately 4500 communities with daily bus service compared to 23,000 communities in 1965 (DMG 2004). Rural areas have unique coordination barriers, including long distances and inefficient land-use patterns, local government financial constraints limiting their ability to pay for transit services, public unfamiliarity with transportation services, and little professional expertise in transportation (Ridout et al. 2008). Sometimes school bus systems are the only means of public transportation in rural areas. These systems can serve as a substitute for public transportation in emergency events as they are widely available in rural areas throughout the nation.

In rural areas, a public transportation fleet size is relatively small, with 2–10 small- and medium-sized vehicles (10–25 passengers' capacity). During routine travel service, transit systems have either a fixed-route system or a demand-response service. A survey conducted by the Western Transportation Institute (WTI) indicates that in an emergency event, transit agencies became more flexible in their transit delivery and provide demand-response service. Passenger assistance levels also increased with higher levels of services such as door-to-door service, package assistance from drivers, the provision of personal care attendants or escorts, and permission for passengers to travel with pets (Jaydeep et al. 2010).

### **18.2.2 The Role of Public Transportation in Evacuation**

An emergency management plan of any organization generally involves a series of documents, activities, education programs, trainings, mock drills, and stakeholders. A plan can be divided into four tasks: (i) mitigation, developing a plan to reduce damage, loss, and impact; (ii) preparedness, developing a plan for readiness; (iii) response,

developing a plan for action/operation; and (iv) recovery, developing a plan for resuming normalcy. Public transportation can perform multiple roles in evacuation and be a successful partner in these four tasks of emergency management plans:

(a) *Mitigation*:

- Protect its own assets (e.g., moving transit vehicles to a safe place during severe flooding and fire incidents).
- Establish redundant communication systems.

(b) *Preparedness*:

- Help in preparing local emergency management plans.
- Represent the various modes of transportation in the emergency command structure.
- Prepare its vehicles to be supplied on demand to law enforcement and EMAs for nontransit purposes.

(c) *Response*:

- Evacuate vulnerable, transit-dependent populations.
- Transport emergency personnel, volunteers, and equipment to an incident site.
- Provide temporary shelter for evacuees.
- Transport food, fuel, and other supplies.

(d) *Recovery*:

- Resume normal service as quickly as possible.
- Move transit-dependent evacuees to their original locations or other destinations.
- Help supply real-time information on the extent of damage (Balog et al. 2005; White et al. 2008).

### 18.2.3 Public Transportation Systems in Evacuation Operations

Before 2005, public transportation operators in the United States did not take the lead on evacuation planning, nor were they viewed as a viable option for evacuation. Hurricane Katrina, and to some extent the 9/11 terrorist attack on the World Trade Center, became the impetus for investigating the role of transit in evacuation and emergency events. Since 2005, there is an increased national awareness and interest in the role of public transportation in evacuation. Typically, EMAs such as police, fire, and emergency medical services—the first responders to an incident—take the lead in an evacuation. However, public transportation can perform multiple roles in evacuation. In evacuation-prone areas, public transportation systems are a successful partner in executing functional local emergency operations plans (EOPs) that involve all modes of transportation. During emergency events, public transportation systems are placed under a local emergency operation center (EOC) and provide specific functions and services that are identified in local EOPs and detailed in transportation system plans and procedures (Jaydeep et al. 2010). EOC is a command center where emergency service providers meet and coordinate response, recovery, and resources

during disasters. School bus systems also function the same way as community transportation systems under EOCs. Operating under local EOCs clears a chain of command resulting in adequate coordination among agencies.

#### **18.2.4 Evacuation Practices in Rural Areas**

Evacuation through public transportation systems in rural areas is not reported widely. In 2009, WTI conducted a survey of 24 public, private, and school transportation agencies in the 24 hurricane-prone coastal counties of Florida, Alabama, and Mississippi and four parishes of Louisiana in the Northern Gulf of Mexico (NGM) region. The survey results indicate that a majority of the transit services in rural coastal counties needed 1–12 h to prepare for an evacuation operation. These agencies also identified communication, employee issues, and financial issues that could hamper their evacuation operation.

In 2004, Hurricanes Charley, Frances, Ivan, and Jeanne hit Florida within a 6-week period. Public transit agencies were actively involved in handling emergency events and evacuations in small urban and rural areas. Although Florida had an advanced state of emergency operation management system, a survey conducted for this evaluation on evacuation operations identified several deficiencies and concerns involving communication, coordination, education, specialized needs, finance, passenger statistics, and required resources (Goodwill and Reep 2005).

At the time of an Air Ontario jet crash near Dryden in Northern Ontario, Canada, school buses proved to be beneficial for a small community where buses were the only means of public transportation. The school buses helped to move the injured to a hospital. On the day of the 9/11 terrorist attacks, school buses helped transport 6600 passengers from an airport to shelters in Gander, Newfoundland, Canada. The buses also helped in recovery operations moving the passengers back to the airport (Scanlon 2005).

#### **18.2.5 Actions Implemented for Emergency Evacuation of Rural Areas**

After lessons learned from hurricane events, terrorist attacks, and wildfire and flood emergency evacuations, transportation agencies launched aggressive programs focused on transit personnel, emergency management officials, and citizens for the emergency management needs of rural transit systems. The following actions are being implemented across the United States:

*Actions 1:* Increasing awareness of transit's role and the critical issues related to mitigation, preparedness, response, and recovery

*Actions 2:* Preestablishing institutional relationship/mutual aid agreements among transit authorities, transportation departments, emergency and law enforcement agencies, emergency responders, healthcare facilities, and the media

*Actions 3:* Conducting regular emergency management planning exercises, education programs, training programs, and mock drills

*Actions 4:* Establishing communication and job responsibility protocols for transit employees

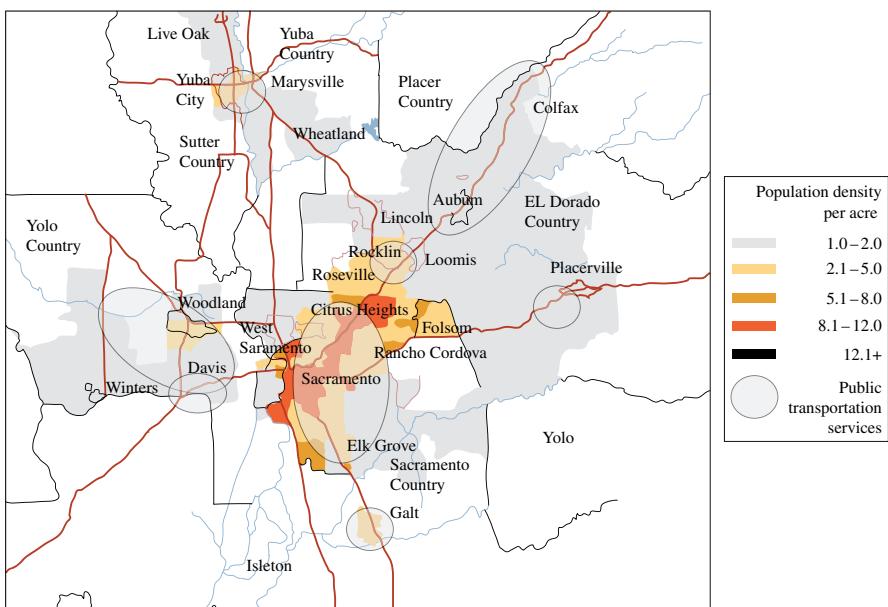
*Actions 5:* Encouraging an environment supporting sustained information sharing and routine interaction among agencies that manage transportation systems

*Actions 6:* Identifying areas of improvement for rural transit including safety, security, and reliability before, during, and after emergencies and determining steps for improvement (Balog et al. 2005; Goodwill and Reep 2005; Communiqué USA 2008a, 2008b; Jaydeep et al. 2010)

### 18.3 SACRAMENTO REGION EMERGENCY RESPONSE CASE STUDY

The Sacramento region consists of El Dorado, Placer, Yuba, Sutter, Yolo, and Sacramento counties. A majority of this region is rural and has very low population densities (Fig. 18.1) except Sacramento county and some parts of Placer, Yuba, and Sutter counties (nearly 1.3 million urban populations).

The Sacramento region faces a number of potential emergency situations caused by flooding, forest fires, earthquakes, and other events. Many parts of Sacramento, Yolo, and Yuba counties are in 100-year flood plains due to the numerous natural bodies of water and vulnerable levees (SACOG 2009c). Natural emergencies pose challenges to this region, especially in rural areas that face frequent threats from fires and floods. For example, nearly 300,000 acres of land and numerous homes were



**FIGURE 18.1** Transit services and population density in the Sacramento region (*Source:* SACOG 2008).

burned in the 2008 California fire (SACOG 2012). Placer and Yuba counties had significant fires, with over 1000 acres burned. Rural infrastructure is more vulnerable to flood events. Many rural roads are composed primarily of dirt and gravel, leaving them suspect to washing out during major floods. Rural emergency services are relatively slow in response times compared to those in urban areas. Citizens who are in nursing homes or hospitals, are unable to drive, or are without a car are at risk and are often left behind in an emergency event.

In the Sacramento region, public transit is concentrated in the densest areas, with 40% of Sacramento Regional Transit's buses serving downtown Sacramento. Overall, 73% of transit routes fall within an urban area and less than 14% serve rural areas (SACOG Expanding Travel Choices for Rural Mobility 2009a) (Fig. 18.1). In addition to local transit providers, supplementary bus service is offered by Amtrak.

### **18.3.1 Public Transportation in Emergency Evacuation and Mock Drill Exercise**

Transit vehicles cannot only move people to safer areas but also provide the opportunity to transport necessities to disaster sites and provide mobile cooling stations for fire-fighters. The role of transit in the Sacramento region has been enhanced through emergency events in the last 13 years. Two major events contributing to the improvement are worth noting. The first emergency event occurred in Yuba and Sutter counties on January 1, 1997, after a massive snowfall before Christmas followed by warm, heavy rain. Voluntary evacuations were ordered on New Year's Day for urban areas in both counties. However, Yuba–Sutter Transit was not notified or given evacuation orders by either EOC. Fortunately, one transit analyst happened to find out about the order and contacted the responsible emergency services official and prepared Yuba–Sutter Transit for the evacuation. Yuba–Sutter Transit split the number of buses in each county so that half of the fleet would remain available for regular services, as well as an expansion of evacuation operations. The buses transported evacuees to schools and community centers in Nevada and Plumas counties of the region. Over 1000 individuals were evacuated by bus drivers and volunteers.

This emergency event exposed several issues faced by the rural transit operators: (i) Yuba–Sutter Transit did not have an open communication with the local EOCs; and (ii) Transit's role in emergencies was not preestablished. The transit agency could have started evacuations earlier, and the expensive evacuation through private ambulance companies could have been avoided if the emergency service officials and the transport operator were in regular contact. If transit operators were included in the jurisdiction's emergency planning, EOCs' officials could have knowledge of transit inventory, accessed the inventory, and remained in contact with transit operators to provide timely service. In response to these issues, many improvements have been made, including frequent communication between the transit operators and emergency planning agencies.

In October 2007, SACOG conducted a mock drill for the region's transit providers and several other emergency agencies to ensure that an emergency response mechanism was in place in case of an evacuation. The full-scale emergency exercise was

funded by the Department of Homeland Security. This exercise was conducted to examine how transit resources could be used to deal with various aspects of a flood emergency, including a levee break. The exercise tested the following areas:

- Interaction between agencies and EOCs
- Coordination among transit operators
- EOC communications of local transit aspects of city and county evacuation plans
- Operational aspects of a mass evacuation

The exercise was very beneficial in both identifying areas where the teams performed well and areas for improvement. An action report (AAR) based on the 1997 evacuation and the 2007 mock drill identified issues in three areas: communication, leadership, and training. A communication mechanism was broke down because the communication plan of the EOC and transit agencies was not completely developed and accurate. This resulted in a delay in the decision-making process and resource tracking. Further, the EOC leadership had never worked with the transit agencies and was not well aware of their function. Due to a lack of EOC procedures and system training, transit operators were not able to assist the EOC on the emergency operation effectively.

### **18.3.2 Actions to Improve Transit Operation Effectiveness in Emergencies**

After identifying various issues in the 1997 evacuation and the mock drill exercise of 2007, SACOG implemented the following multiple initiatives based on the AAR recommendations:

1. SACOG began working on a plan to improve emergency-related communications, evacuation procedures, and information for transit agencies and local EOCs. This plan was funded by the California Department of Transportation (Caltrans).
2. SACOG set up an advisory group—the Transit Coordination Committee. This group was given responsibility to study flooding effects on the region's transit systems, oversee future mock drills and actual evacuation operations, and prepare the region for meeting any emergency needs.
3. SACOG began working with Caltrans and other organizations to implement an intelligent transportation system (ITS) project called the Sacramento Transportation Area Network (STARNET) system, a 511 website, and an interactive telephone service (dial 511). This system was expected to allow real-time information access to transit agencies and local EOCs for better coordination in providing transit services in emergencies (SACOG 2009b).

In addition to the above actions, Caltrans launched regional workshops on emergency management for rural and small urban transit operators, emergency officials, law enforcement, and other emergency responder agencies. The goal of the project was to support emergency planning efforts for rural and small urban transit agencies, to improve interagency communication and coordination, and to provide training on leadership, emergency plans and procedures, and communication equipment.

## 18.4 HURRICANE SANDY COASTAL COUNTIES EVACUATION CASE STUDY

Hurricane Sandy was the most destructive of the 2012 Atlantic hurricane season and the second most expensive hurricane in United States history. Hurricane Sandy affected 24 states, including the entire eastern coast from Florida to Maine and west across the Appalachian Mountains to Michigan and Wisconsin, with particularly severe damage occurring in New Jersey and New York. Its storm surge hit New York City on October 29, flooding streets, tunnels, and subway lines and cutting power. Damage in the US is estimated around \$50 billion (Blake et al. 2013).

Hurricane Sandy's hardest hit were the communities of the Jersey Shore throughout the tristate region. Public transit agencies of Monmouth, Ocean, Atlantic, and Cape May counties of New Jersey played a significant role in the emergency even as they prepared for the return of their regular services and focused on populations without access to an automobile or traditional bus and rail services under the leadership of their offices of emergency management (OEM). Table 18.1 lists the series of actions taken during the evacuation operation by the transit agencies.

Transit agencies and the OEM had prior experience of evacuation during Hurricane Irene in 2011. Almost all agencies experienced their dual role in balancing needs of regular daily services and emergency mobility demand. The most important lesson

**TABLE 18.1 Hurricane Sandy Evacuation Operation of Coastal Counties of New Jersey**

Timeline	Action
Before the storm	Individual county OEM gave the advance notice to all transit agencies and asked to scope out the role of transit agencies. A series of meetings were held to sort out evacuation details. Transit staff approached local hospitals and requested all appointments to be completed before hurricane arrival. The vehicles were called in to OEM command centers
Hurricane eve (October 28, 2012)	Transit agencies began early evacuation to local county emergency shelters and reception centers
Hurricane arrival (October 29, 2012)	Last-minute evacuation requests were responded to and meal services were completed before Hurricane Sandy hit land in the afternoon. Evacuation operation was closed for a day
After hurricane (October 30, 2012)	Transit drivers provided bulk meal deliveries to the shelters and shifted evacuees from reception centers to main evacuation centers
Normalcy day 2 (October 31, 2012)	Transit services continued to provide bulk meal transports, and evacuees were transferred to the main shelter. Some medical transportation services were provided
Normalcy day 3 (November 1, 2012)	New services such as transporting evacuees back to their homes where possible, providing nonmedical transportation needs, meal services to nursing homes, and food shopping services were launched. Citizens who lost homes were provided transportation to alternate arrangements made by OEM

*Source:* Adapted from Fittante (2013).

learned by the transit agencies was to establish a close working relationship with the OEM and adjacent counties' transit systems. However, transit agencies persistently battled with transit drivers. In Atlantic and Ocean counties, almost 50% of the transit agencies' drivers were victims of heavy flooding and could not return to work. This issue, to some extent, hampered the evacuation efforts.

## 18.5 CONCLUSION AND FURTHER DISCUSSION

The objective of this chapter was to investigate what role public transportation systems played, how adequately transit systems were prepared, and identify what challenges and issues existed in the event of an emergency/evacuation in rural areas. To provide some context for this, the study began with a review of available literature on the role of transit in emergency evacuations. Issues, concerns, recommendations, and best management practices are discussed in several research reports and articles for the purpose of improving transit operation during emergency events. Some recommendations that have been put forth in these materials include improving coordination among agencies, conducting regular mock disaster drills, increasing participation of citizens and transit, and establishing mutual aid agreements. Many of these activities are incorporated into rural evacuation practices in the Sacramento region. Experiences during Hurricanes Katrina, Rita, and Sandy (the worldwide known disasters) and the emergency events in the region may have impacted and had a lasting influence on emergency preparedness. Transit agencies also demonstrated capabilities to provide emergency services to their respective service jurisdiction in the wake of severe storms, floods, and tornados. The capabilities include increasing level of passenger assistance and flexibility in service, scheduling, delivery, and jurisdiction. However, discrepancies in emergency operations require improvement to make evacuations more efficient and effective. For example, the case study indicates that communication, leadership, and training were major issues for the Sacramento region. The survey conducted by WTI for the NGM region and the case studies indicate that there are technical issues in communications, employee issues, and finance that present major stumbling blocks in conducting emergency operations and will require further study to make emergency operation more efficient and effective.

### 18.5.1 Communication

In addition to institutional communication issues such as regular meetings, task force meetings, and planning workshops, technical issues, such as sparse communication network coverage in rural areas or network breakdown during an evacuation operation due to conditions such as flood, rain, wind, power outages, large geographical area, or dense vegetation, play a critical role in the coordination of emergency operations. Use of satellite phone technology, a mobile communication briefcase, and reliable passenger information would be a reliable, effective, and efficient way for transit agencies to enhance and ensure information dissemination.

### **18.5.2 Employee Issues**

Transit employees are the most valuable assets for agencies during an evacuation operation. One of the most critical issues identified in the survey and case studies was that more than 50% of employees did not report to work on the last evacuation call. This issue was most prevalent within the largest segment of the transit agency workforce—its drivers. Drivers are responsible for carrying out routine and evacuation transit operations. An issue that prevented employees from reporting for work was concern for the safety of themselves and their families. Transit agencies attempted to address this issue by offering compensation to employees, sheltering families at secured facilities, and giving notice and time to prepare for the needs of their families. Agencies also faced a more fundamental problem in simply establishing communication with employees for post-emergency event operations.

Employee roles and responsibilities in emergency events should be well defined in the job description and reinforced with essential job training. A “prior commitment” form clarifying expectations could be signed by employees during the hiring process, along with notification of defined emergency assistance benefits for serving in emergency events. Some of the agencies did not train their employees in areas that would enhance transit services in rural areas, such as:

- Serving people with limited English proficiency
- Serving people with service animals or pets
- Incident command system management
- Emergency communication
- Driving in hurricane traffic zones

### **18.5.3 Inadequate Finances**

Funding for evacuation-related operations and capital expenses for transit was the most significant and frequently cited concern related to emergency planning that was found during the WTI survey. Transit agencies in the NGM indicated this was an issue in three different categories of the survey: (i) employee issues, lack of budget for compensation or overtime; (ii) transit revenue and expenditure; and (iii) assessment of needs/coordination, barriers/obstacles. Transit agencies reported that they were having issues with lack of operating budgets, restricted funding, and billing and payment as barriers/obstacles for providing emergency services.

In the authorization of a new transportation bill, it is suggested that Congress recognize the funding issues related to evacuation operations and authorize the Federal Transit Administration (FTA) or the Federal Emergency Management Agency (FEMA) to reimburse transit evacuation expenses including operation, training, and preparation. Reimbursement may be extended to purchase communication devices and ITS equipment to enhance evacuation operation capabilities. States can leverage taxes on flood and natural disaster insurance policies to fund emergency management activities.

In rural areas, school buses are sometimes the only means of public transportation. School bus systems are a critical resource because they are safe, reliable, and readily available for rural evacuation operations. However, this critical resource is not being explored for emergency events. In order to use school buses, the following advantages and disadvantages should be considered during emergency management planning:

1. Advantages:

- School bus systems routinely deal with issues such as altered bus schedules, traffic congestion, and weather conditions.
- Bus drivers, operational equipment, and buses are ready to perform multiple tasks in emergency events.
- In many instances, schools are being used as shelters; therefore, it would be more convenient for school bus systems to coordinate an evacuation operation.
- School buses are painted yellow, which would be beneficial for law enforcement agencies in giving them priority consideration in traffic and for passengers to identify their evacuation vehicle.
- Useful school district resources such as school nurses, safety officers, coordinators, and mechanics could be available to supplement emergency operation personnel.

2. Disadvantages:

- Compared to public transportation buses, school buses have limited wheelchair-accessible spots.
- School buses are not equipped with air conditioning, which may cause inconvenience for some passengers.
- School buses have to rely on local EMAs for passenger information, maps, and directions to pickup locations and shelters.
- If school bus systems are not incorporated into a local emergency management plan, their utilization and response time during an emergency may be significantly delayed.
- The regular school bus capacity is between 20 and 76 students. Adults take up significantly more space on a school bus than children, and therefore, capacity would be considerably reduced in evacuation.
- School buses may be at greater risk of exposure to litigation for inconvenient service during an evacuation because the buses may not be covered under insurance for evacuating general public.

## REFERENCES

Balog, John N., Annabelle Boyd, Jim Caton, Peter N. Bromley, Jamie B. Strongin, David Chia, and Kathleen Bagdonas. 2005. *Public Transportation Emergency Mobilization and Emergency Operation Guide*. TCRP Report 86. Washington, DC: Transportation Research Board.

- Blake, Eric S., Todd B. Kimberlain, Robert J. Berg, John P. Cangialosi, and John L. Beven II. 2013. *Tropical Cyclone Report: Hurricane Sandy*. National Climatic Data Center: National Oceanic and Atmospheric Administration. Retrieved from [http://www.nhc.noaa.gov/data/tcr/AL182012\\_Sandy.pdf](http://www.nhc.noaa.gov/data/tcr/AL182012_Sandy.pdf) (accessed on March 30, 2013).
- Committee on Nationwide Plan Review Phase 2. 2006. *Nationwide Plan Review Phase 2. Report to Congress*. Washington, DC: The Department of Homeland Security (DHS) and the Department of Transportation.
- Communiqué USA. 2008a. *Rural Transit Response and Recovery Conference—After Action Report*. Division of Mass Transportation, Caltrans, March 3–4, San Diego; March 6–7, Monterey; and March 10–11, Sacramento. Retrieved from [http://www.dot.ca.gov/hq/MassTrans/Docs-Pdfs/aar08\\_final.pdf](http://www.dot.ca.gov/hq/MassTrans/Docs-Pdfs/aar08_final.pdf) (accessed on February 25, 2015).
- Communiqué USA. 2008b. *Rural Transit Emergency Planning Guidance. Guidance Document*. Sacramento, CA: Division of Mass Transportation, Caltrans.
- Dye Management Group (DMG) Inc. 2004. *Planning for Transportation in Rural Areas*. Retrieved from [http://www.fhwa.dot.gov/planning/publications/rural\\_areas\\_planning/](http://www.fhwa.dot.gov/planning/publications/rural_areas_planning/) (accessed on January 18, 2011).
- Fittante, Steve. 2013. *Community Transit Demonstrates Its Value in Response to Hurricane Sandy*. Community Transportation Magazine of the Community Transportation Association of America. Retrieved from [http://web1.ctaa.org/webmodules/webarticles/articlefiles/Dec\\_12\\_DigitalCT\\_Sandy.pdf](http://web1.ctaa.org/webmodules/webarticles/articlefiles/Dec_12_DigitalCT_Sandy.pdf) (accessed on March 30, 2013).
- Goodwill, Jay A. and Amber, Reep. 2005. *Transit Emergency Planning and Response Assessment Initiative*. Research Report. Tampa, FL: Center for Urban Transportation Research, University of South Florida.
- Jaydeep, Chaudhari, Janelle Booth, Zhirui Ye, David Kack, Benedict Posadad. 2010. Evacuation Preparedness of Public Transportation and School Buses In Rural Coastal Communities of the North Gulf Region. Retrieved from [http://www.westerntransportationinstitute.org/documents/reports/4W2643\\_Final\\_Report.pdf](http://www.westerntransportationinstitute.org/documents/reports/4W2643_Final_Report.pdf) (accessed on February 25, 2015).
- Ridout, J. S., Annie E. Dunning, Berry C. Nocks, James B. London, Angela Mathias, and Elinor Hiltz. 2008. Transportation Service Coordination in a Rural State. Proceedings of the Transportation Research Board 2008 Annual Meeting (CD-ROM), Washington, DC, January 13–17, 2008.
- SACOG. 2009a. *Expanding Travel Choices for Rural Mobility*, Retrieved from <http://www.sacog.org> (accessed on September 19, 2009).
- SACOG. 2009b. August 21. *Rural–Urban Connection Strategy-Sacramento Council of Governments*. Retrieved from [http://www.sacog.org/rucs/wiki/index.php/Main\\_Page](http://www.sacog.org/rucs/wiki/index.php/Main_Page) (accessed on September 17, 2009).
- SACOG. 2009c. *Emergency Response*. Retrieved from <http://www.sacog.org> (accessed on January 31, 2011).
- SACOG. 2012. Metropolitan Transportation Plan/Sustainable Community Strategy-2035. Retrieved from <http://sacog.org/mtpscs/files/MTP-SCS/MTPSCS%20WEB.pdf> (accessed on February 25, 2015).
- Sacramento Council of Governments (SACOG). 2008. *Population Estimates*. Retrieved from <http://www.sacog.org/about/advocacy/pdf/fact-sheets/PopulationStats.pdf> (accessed on September 19, 2009).

- Scanlon, Joseph. 2005. Transportation in emergencies: an often neglected story. *Disaster Prevention and Management*, 12(5):428–437.
- White, Richard A., Evelyn Blumenberg, Kenneth A. Brown, John M. Contestabile, Ali Haghani, Arnold M. Howitt, Thomas C. Lambert, Betty Hearn Morrow, Michael H. Setzer, Ellis M. Stanley, Sr., and Andrew Velásquez III. 2008. *The Role of Transit in Emergency Evacuation*. Special Report 294. Washington, DC: Transportation Research Board.

# INDEX

Note: Page numbers in *italics* refer to Figures; those in **bold** to Tables.

- adaptive resilience
  - challenges, transportation security, 67
  - CI security requirement, 67
  - critical infrastructure protection (CIP), 68
  - definition, 66–7
  - infrastructural preparation, 68
  - national security agenda, 67
  - 9/11 Commission policy recommendation, Homeland Security Act of 2002, 66
  - policy shifts, 68
  - regular and catastrophic risks, 66
  - research and practice
  - structural and policy-level impacts, 68
  - total resilient ecosystem, 68
- ADGP *see* Red Cross Annual Disaster Giving Program (ADGP)
- airport security policy, cost-effective antiterrorism security, 224
- Aviation and Transportation Security Act (ATSA), 205
- aviation security, 206–9
- Canada, risk-based policy, 210–211, 225
- Canadian Air Transport Security Authority (CATSA), 221
- compensation levels, airport screeners, 224
- Europe’s steps toward risk assessment, 211, 225
- Federal Aviation Administration (FAA), 222
- International Civil Aviation Organization (ICAO), 209–10
- mode specific, EU countries, 225–6, 227
- “one-stop” security for intra-EU passengers, 226
- paying, airport security, 224–7
- policy decisions, 219
- provision in Europe, 2011, 219–21, **220–221**
- risk-based approach, 213–19
- Transportation Security Administration (TSA), 205, 222–3
- TSA-screened Los Angeles International (LAX), 223
- United Kingdom, 225

- airport security policy, cost-effective (*cont'd*)  
 United States  
   airport screening, 224  
   behavior detection officers (BDOs), 227  
   in-line screening, 226  
   TSA funding, 227
- ALARA *see* as low as reasonably achievable (ALARA)
- American freight railroad system, post-9/11  
 access control and trespassers, 191  
 chlorine gas and ammonium, 191  
 Class I railroads, 191  
 computer platforms, 191  
 economic growth, 189–190  
 foot-and-mouth disease, 190  
 globalization, 189  
 Italian freight train, 191  
 observations  
   computer networks, 196–7  
   corporate security, 195  
   data collection, 193  
   environmental risk, 196  
   food supply chain, 197  
   general systems theory, 192  
   investigator, inspections, 193  
   nature and geographical location, 195  
   nonrandom sampling frame, 192  
   physical barriers, 197  
   potential security risks, 195, 196  
   private property, 193  
   rail switches, 194  
   security management, 194  
   stakeholders, 192  
   tank cars and hazardous materials, 194–5  
   toxic-by-inhalation chemicals, 196  
   trespassers, 193–4  
   weapons of mass destruction (WMD), 196
- passenger rail, 190  
 power production, 190  
 security management and  
   counterterrorism, 197–201
- American Public Transportation Association (APTA), 184
- areal contamination, assessment  
 decontamination, 127  
 disposition of victims, 126  
 stabilization, 126
- as low as reasonably achievable (ALARA), 121–3
- ATS *see* Automated Targeting System (ATS)
- ATSA *see* Aviation and Transportation Security Act (ATSA)
- Australia, rising heat  
 Black Saturday, 320, 327  
 bushfires, 319, 320  
 emergency preparedness and response  
   incident command, 322–4  
   local government, 324  
   Stay or Go policy, 320, 322  
 evacuation policy  
   hospitals, 326  
   vulnerable populations, 326  
 events timeline, 320, 321
- Automated Targeting System (ATS), 246
- Aviation and Transportation Security Act (ATSA), 205
- aviation security measures  
 challenges, terrorism  
   asymmetries, 206  
   benefit/cost (B/C) analysis, 206  
   Gross Domestic Product, 206–7  
   monetary benefits, terrorist act  
   prevention, 206  
   safety analysis and security, 207  
   sector-specific approach, 206
- cost-effectiveness analysis  
 federal air marshals (FAMs), 207–8  
 Federal Aviation Administration (FAA), 207  
 9/11 attack, 208  
 relative effectiveness, 208–9  
 TSA aviation security efforts, 207
- BC *see* betweenness centrality (BC)
- behavior detection officers (BDOs), 226
- BENS *see* Business Executives for National Security (BENS)
- betweenness centrality (BC)  
 definition, 36–7  
 vs. traffic flow  
   augmented variants, 42–3  
   mobility-oriented BC, 47  
   nodes, correlation, 43, 46, 47  
   origin–destination (OD), 42, 44  
   peak hours, 44–5, 45  
   power law distribution, 42, 43

- shortest path assumption, 44  
squared error (*R*<sup>2</sup>), free-flow traffic fraction, 45  
stub and transit nodes, 45–6  
transportation network, 37  
British Transport Police (BTP), 157  
broken window theory, 163  
Business Executives for National Security (BENS), 7, 10
- The Call for a Global Islamic Resistance*, 29
- Canada, risk-based policy  
Canadian Air Transport Security Authority (CATSA), 210  
Canadian Air Transport Security Program (NCASP) document, 211  
Registered Traveler (RT) program, 210  
risk-based approach, 210  
Trusted Traveler (TT) program, 211
- CBRN *see* chemical, biological, radiological and nuclear (CBRN)
- CFA *see* Country Fire Authority (CFA)
- chemical, biological, radiological and nuclear (CBRN), 137, 139
- concept of operations (CONOPS), radiation detection  
areal contamination, 125–7  
Cs-137 gamma-ray, 122  
KINT *see* knowledge intelligence (KINT)  
limits, contaminated region, 127  
as low as reasonably achievable (ALARA), 121–2  
metro station, 125  
nuclear weapon, 122  
sensors, 125  
static source  
control, establishing, 123  
detection, confirmation, 123  
locating, 123  
safety perimeters, 123  
sensitivity and cost, trade-off, 122  
unmanned ground vehicle (UGV), 123–4  
tracking, moving source, 124–5  
training officers, 122
- Container Security Initiative (CSI), 246
- Country Fire Authority (CFA), 322–4
- crime prevention through environmental design (CPTED), 163, 165, 168, 170
- CSI *see* Container Security Initiative (CSI)
- C-TPAT *see* Customs–Trade Partnership against Terrorism (C-TPAT)
- Customs–Trade Partnership against Terrorism (C-TPAT), 198, 201, 246
- cyberterrorism  
commuter lines and regional railroads, 5  
concept, 5  
cyberattacks, 6  
cybersecurity, 6  
information and communication technologies (ICT), 5  
signaling, computer-based, 5
- DAS *see* distributed acoustic sensing (DAS)
- defensive intelligence, 117
- Department of Homeland Security (DHS), 205, 209, 212, 216, 227
- Department of Sustainability and Environment (DSE), 322–4
- depth first branch and bound (DFBnB), 48
- deterrent intelligence, 117, 118
- distributed acoustic sensing (DAS), 302–3
- drones, 301–2
- environmental design, transit security  
crime prevention through environmental design (CPTED), 163, 165, 168  
glass, 168  
natural surveillance, 163  
physical characteristics, stations, 163, 165  
security-oriented design strategies, transit stations, 165–7, 170  
Stockholm tram, clear sightlines, 163, 164
- e-RAILSAFE program, 199
- evacuation *see also* evacuation plan  
definition, 346  
emergency  
actions, rural areas, 367–8  
Australia *see* Australia, rising heat  
evacuation order, 318  
factors, influencing, 319  
institutional partnerships, 319  
Japan *see* Japan, multihazards  
law enforcement, 318  
procedures and information, 318  
“shelter in place,” 319
- emergency planning and response, 7
- innovations, 7

- evacuation *see also* evacuation plan (*cont'd*)  
 jurisdiction features, 6  
 mandatory orders  
   Hurricane Irene, 351  
   Hurricane Katrina, 348  
   Hurricane Sandy, 352  
 procedure, 7  
 transportation infrastructure, 6
- evacuation plan  
 components, 346, **347**  
 definition, 346  
 Irene  
   Atlantic City, 350  
   buses, 351  
   mandatory evacuation order, 351  
   NJ Transit, 351  
   post-Irene emergency preparedness conference, 351  
   shelters, 351  
 Katrina  
   communications problem, 348  
   delayed response, 348  
   Internet and social media, 348  
   mandatory evacuation order, 348  
   National Response Plan (NRP), 346  
   shelter, 349  
   Southeast Louisiana Catastrophic Hurricane Plan (SLHCP), 349  
   successes, 349  
 "preferred" plan, 346  
 Rita  
   automobile traffic problems, 350  
   resident's response, 349  
 Sandy  
   damages, 352  
   mandatory evacuation, 352  
   refusal, evacuation, 352  
 suggestions  
   development, vulnerable areas, 356–7  
   interaction, emergency and transportation officials, 353  
   modern technology incorporation, 354–5  
   preparedness, attention and resources, 353–4  
   private sector involvement, 357–9  
   resistance to evacuation, 355–6  
   special needs population, 355
- FBI *see* Federal Bureau of Investigation (FBI)  
 FBI National Joint Terrorist Task Force (JTTF), 198  
 federal air marshals (FAMs), 207–8, 213  
 Federal Aviation Administration (FAA), 207, 222  
 Federal Bureau of Investigation (FBI), 154, 162  
 Federal Emergency Management Agency (FEMA), 183–5  
 foot-and-mouth disease, 190
- GAO *see* Government Accountability Office (GAO)  
 GBC *see* group betweenness centrality (GBC)  
 Geiger–Müller (G–M) detector, 111–13  
 German Red Army Faction (RAF), 27  
 GF program *see* Green Field (GF) program  
 G–M detector *see* Geiger–Müller (G–M) detector  
 Government Accountability Office (GAO)  
 Federal Emergency Management Agency (FEMA), 184  
 surface transportation security inspectors (STSIs) program, 183, 185  
 greedy algorithm, 48, 49, 53  
 Green Field (GF) program, 132  
 Gross domestic product (GDP), 206, 207  
 group betweenness centrality (GBC)  
   depth first branch and bound (DFBnB)  
   greedy algorithm, 48  
   homeland security threats, 47  
   net number, vehicles, 48  
   search algorithms, 49, 50  
   solution, time bound, 49, 51  
   traffic monitors, 48–9, 49
- Hezbollah, Shiite organization, 27  
 hijacking, terrorist-motivated attacks on trains, 28  
 civil aviation targets, 26  
 commercial aircraft, 26  
 deal with terrorists, 27  
 firearms, infiltration in aircraft, 27  
 freeing prisoners, goal of, 26  
 Islamist terrorism, 27  
 Japanese Red Army (JRA), 26  
 left-wing terrorist groups, 27

- Libya, attacks from, 27–8  
material benefit, 26–7  
9/11, 28  
“skyjacking,” 26  
standing operation procedures  
(Israeli Air Force), 28
- Homeland Security Act of 2002, 66
- Hurricane Sandy coastal counties  
evacuation  
actions, operation, 371, **371**  
offices of emergency management  
(OEM), 371  
transit agencies, 371, 372
- IAEA *see* International Atomic Energy Agency (IAEA)
- ICAO *see* International Civil Aviation Organization (ICAO)
- IFSAR *see* interferometric synthetic aperture radar (IFSAR)
- improvised nuclear devices (INDs), 116–17, 125, 127
- Incident Management Teams (IMTs), 324, 325
- information and communication technologies (ICT), 5
- information management, pipeline security  
data and information sources  
documentation, 291  
external data sources, 291  
operators, 292
- geopolitical information, 290–291
- open *vs.* confidential information, 292–3
- physical characteristics  
general system, 289  
segment, 289, 290  
transported product, 290
- Information Sharing and Cooperation (ISACs), 162, 198
- Integrated Emergency Coordination Centre (iECC), Melbourne, 322, 324
- intelligent transportation system (ITS), 370
- interferometric synthetic aperture radar (IFSAR), 301
- International Atomic Energy Agency (IAEA)  
categories, radionuclides, 130, 131  
contaminated areas, 142  
isotopes, 110  
radioactive materials, 129–30
- International Civil Aviation Organization (ICAO)  
aviation security, 209  
Standard 3.1.3 of Annex 17, 209–10
- Intifada (2001–2004), 28
- Iraqi Sunni Association of Muslim Scholars, 32
- ISACs *see* Information Sharing and Cooperation (ISACs)
- Israeli network, attack scenarios (case study)  
normalized benefit, monitoring system, 58  
optimal number of monitoring units, 57  
scenarios  
limited threat, 56  
local threat, 56  
metropolitan threat, 56  
regional threat, 56
- ITS *see* intelligent transportation system (ITS)
- Japanese Red Army (JRA), 26
- Japan, multihazards  
earthquake disaster, 328  
emergency preparedness  
failures, chain of command, 329–30  
nuclear emergency response structure, 329, 329  
and public safety, 336–7
- evacuation  
communication, evacuees and public reaction, 332–3
- Futaba, 334
- hospitals, 335–6
- older adults, 336
- orders, 330, 331
- prefecture government and local municipalities, 330, 332
- Tomioka and Kawauchi, 334
- vulnerable populations, 334–5
- nuclear disaster, 327–8
- “The Jihad of Iraq—Hopes and Dangers” (document), 31
- knowledge intelligence (KINT)  
accuracy and reliability, 118, 119  
actionability, 119–20  
layered system, 120–121  
Pacific War, 119  
timeliness, 118, 119

- Lawrence Livermore National Laboratory (LLNL) technology, 241
- locations, surveillance and monitoring stations
- combinatorial optimization techniques, 48
  - deployment, monitoring systems, 48–9
  - depth first branch and bound (DFBnB)
    - heuristic search algorithm, 48
  - greedy algorithm, 48
  - group variant, shortest path betweenness centrality (GBC), 47–8
  - potential search, 48
  - time, search algorithms, 50
  - total net traffic flow, 49
- Los Angeles International (LAX), 223
- Maritime Transportation Security Act (MTSA), 246
- mass transportation attacks, Islamic justification
- condemnation and *fatwas*, statements, 32–3
  - hostages or prisoners of war, jihadi principles, 31
  - Islamic law (*Shari’ah*), 29
  - jihadi ideologues, 31–2
  - legal ruling (*fatwa*), 29
- London Underground bombings (7/7/2005) (Abu Musab al-Suri), 30
- 1998 fatwa (Bin Laden), 29
- revenge and eye for an eye, principle in jihad, 32
- value of bombing planes, 30–31
  - “weak link,” Western alliance, 31
  - Western economy, disruption of, 30
- Megaports Initiative of the National Nuclear Security Administration, 247
- mock drill exercise, rural evacuation, 369–70
- National Employment Law Project (2009), 263
- National Incident Management System (NIMS), 353
- National Israeli Transportation Planning Model
- biconnected components, 39
  - congestions
    - definition, 40
    - power law distribution, 40
  - Wardrop’s user equilibrium*, 40
- flow through nodes
- inbound flow, distribution of, 41
  - incoming vs. outgoing, 41
- network structure, properties, 39, 39–40
- structurally equivalent vertices, 39
- National Response Plan (NRP), 346
- networks (transportation), defense
- BC *vs.* traffic flow *see* betweenness centrality (BC)
  - “collaborative monitoring units deployment problem,” 37
- computer communication networks, 37
- dataset
- cellular phones, penetration, 38
  - Israeli model *see* National Israeli Transportation Planning Model
  - travel behavior, study of, 39
- deployment schemes, 36
- household survey data, 36
- mobility-oriented BC, 59
- mobility patterns, prediction of, 37
- monitoring stations, 36
- nonresponse to surveys, 36
- optimizing locations *see* locations, surveillance and monitoring stations
- origin-destination (OD) overlay, 37
- for policy-makers *see* policy-makers, networks defense applications
- protein interaction networks, 37
- rationality criterion, 37
- related work
- hazardous materials, monitoring, 38
  - homeland security, 38
  - infrastructure, 38
- neutron detector materials, 114
- NIMS *see* National Incident Management System (NIMS)
- North American Free Trade Agreement (NAFTA), 190
- OD *see* origin–destination (OD)
- OECD/International Transport Forum Round Table on Security, Risk Perception, and B/C Analysis, 208, 207
- offensive intelligence, 117, 118
- Olympic Munich massacre (1972), 27
- onionskin principle, 304
- open-air intrusion detection sensors, 299–300
- Operation Safe Commerce (OSC), 246

- opportunity cost, 206  
origin–destination (OD), 42, 44  
Oslo Agreement (1993–1996), 28
- Palestinian Liberation Organization (PLO), 26  
Palestinian Popular Front for the Liberation of Palestine (PFLP), 27, 28
- peak time demand, 8  
perceptions (travelers) of security, long-distance travel  
high-speed rail (HSR) networks, 92  
information, Foreign and Commonwealth Office, 92
- Italian case study  
behavioral travel/mode choice patterns/security changes, 100–102  
frequency, transport mode use, 99, **99**  
government enforcement, privacy, and security efforts, 102–4  
last/current long-distance trip, description, 99, 99–100, *103*  
perceptions and attitudes, security issues, *102, 103*  
perceptions, security level of transport modes, *100*  
sample and travel behavior features, 97–9  
socioeconomic data, overview, 98  
survey description and design, 97
- literature review  
control measures, perceived, 95  
determinants, threats' perceptions, 93  
latent variable choice model, ordered attitudinal indicators, 94  
local or urban transportation behavior, 95  
national and global level, perceptions of threats, 94  
National Security Strategy, 94  
positive impressions, 94  
real and perceived risks, 93  
results, effects of terrorist threats survey, 95  
user attitudes, role of, 94  
users react, types, 94–5  
views, security levels, 94
- methodology  
map of respondents, 96  
questionnaire, 96  
Rome, focus of research, 95–6
- results, 105–6  
security attributes/comprehensions/evaluation by respondents, **108–9**  
security, aviation sector, 91  
security within the EU, 92  
September 11, 92
- perimeter intrusion detection sensors (PIDSs)  
nuisance alarm rate (NAR), 299  
probability of detection (POD), 299  
vulnerability, defeated/bypassed, 299
- PFLP *see* Palestinian Popular Front for the Liberation of Palestine (PFLP)
- PIDSs *see* perimeter intrusion detection sensors (PIDSs)
- pipeline security  
accidents  
serious accidents, 282  
significant accidents, 281  
advanced countermeasures  
drones, 301–2  
open-air intrusion detection sensors, 299–300  
remote sensing systems, 300–301
- information management *see* information management, pipeline security
- integration, security layers, 304
- intentional acts  
cyberterrorism, 288–9  
terrorism, 284–8  
vandalism and sabotage, 283–4
- intentional/malicious acts, 282
- perimeter protection measures, 295–6
- protection from cyberattacks, 304–5
- risk assessment  
activities, 306  
example, 307, **308**  
steps, 306
- technologies  
cost reduction, 303  
distributed acoustic sensing (DAS), 302–3
- terrorist attacks, 293
- traditional countermeasures  
access control, 297–8  
fences, 296–7  
lighting, 296  
patrol, 298–9

- policing, transportation system, 156–7, 171
- policy-makers, networks defense applications
- functions  $f_{BC}$  and  $f_{Sampling}$ , 52
  - normalized benefit, monitoring system, 55
  - optimal monitoring strategy, 53–4, 54
  - overall monitoring probability, 51
  - performance, monitoring method, 52, 53
  - positive correlation, BC of nodes and traffic volume, 50
  - quality, monitors, 51
  - ratio, cost of monitoring unit and successful attack, 54
  - response time, 51
  - trade-off, monitoring units and quality, 52
- port choice model
- estimation results
    - additional waiting time and travel cost, 276
    - mixed binary logit model, 276, **276**
    - sigma panel coefficient, 277
  - specification, 275–6
  - willingness to pay (WtP), 277–8
- port of Chios (case study)
- data collection, 274, **274**
  - security attitudes and perceptions
    - level 1 characteristics, 274
    - overall feeling of security, 275
    - port specific feeling of security, 275
- public private partnership (PPP)
- BENS, 10
  - “built-in” improvement, 8–9
  - buses, 7
  - businesses behavior, 9
  - Business Executives for National Security (BENS), 10
  - council, 12–13
  - energy consumption, 8
  - government’s response, disasters, 10
  - homeland security, 9–10
  - households and businesses, 9
  - monopolistic government, 10
  - monopoly/noncompetition, 8
  - peak time demand, 8
  - private security officers, 11
  - profit-motivated businesses, 10
  - volunteers, 11–12
- radiation detectors
- CCD/CMOS cameras, 113
  - G–M detector, 111, 113
  - scintillators, 111, 113
  - semiconductor, 111, 113
  - types, 111, 112
  - ventilation system, 142
- radiation emitting device (RED), 116, 117, 122, 125
- Radiation Portal Monitors (RPM), 236
- radiation threat scenarios
- attack methodology, 117
  - nuclear weapons and improvised nuclear devices (INDs), 116–17
  - radiation-emitting device (RED), 116, 117
- radiological dispersion device (RDD) attack
- areal contamination, 125–6
  - casualties, 130
  - Goiânia accident, 142
  - indoor explosion
    - buildings, transportation, 136
    - explosions, video camera shots, 136, 138
    - steel chamber, 136
    - TNT explosions, high-speed camera snapshots, 136, 137
  - outdoor explosion
    - activity distribution, GZ area, 133, 134
    - fireball-ground interaction zone
      - snapshots, 133, 134
    - gamma detectors, 133
    - $\text{LaBr}_3$  detector, 133, 135
    - $^{99m}\text{Tc}$ , 132
    - particles, aerosols, 133
    - radiation measurements, 133
    - surface deposition, 132–3
  - quantity of explosives, 143
  - radiation threat scenarios, 116–17
- radiological threat *see also* radiological dispersion device (RDD) attack
- casualties and economic damages, 129
  - economic and physiologic effect, 142
  - explosive detection system, 143
  - IAEA *see* International Atomic Energy Agency (IAEA)
  - personal screening process, 143
  - radiation contamination and exposure, 131–2
  - radiation sources and detection
    - absorbed dose, 114
    - dose rate, 110–111

- effective or equivalent dose, 114  
ionizing radiation, 110–111  
isotopes, 110  
layered system, 120–121  
neutron detector materials, 114  
radioactive decay, 110  
strengths and weaknesses, 120  
units, 114  
radioisotopes, 129–30, 143–4  
size of contaminated area, 131
- rail vulnerabilities, United States  
catastrophic accidents, 177–8  
classification, threats, 180  
hazardous materials, urban areas, 178  
human-caused threats, 180–181  
integrated system of intelligence, 179  
interconnected complex network, 179–80  
intermodalism, 181  
passenger rail and freight rail, 187  
passenger traffic, 178  
policy and programs, 186  
positive signs, 178  
private owners and operators, 180  
rail safety and security, 186  
recommendations, 179  
risk assessment, 187  
security enhancement, steps, 185
- Red Cross Annual Disaster Giving Program (ADGP), 357
- Red House (RH) program, 132, 136, 139, 144
- remote sensing systems  
interferometric synthetic aperture radar (IFSAR), 301  
LIDAR (airborne and satellite radar), 301  
Scanning Hydrographic Operational Airborne LIDAR Survey (SHOALS), 301
- resilience, evacuation planning, 360 *see also* adaptive resilience
- resilient transportation infrastructure  
multihazard design approach, 78  
protection and resilience, 77, 78  
US highway system, 79
- RH program *see* Red House (RH) program
- risk-based approach, airport security policy  
aviation security officials, 213  
checked baggage screening, 218–19
- ordinary and high-risk passengers  
separation, 217
- passenger and baggage screening  
body scanners, 214  
high-risk passengers, 215  
hijackers, boarding, 214  
low-risk passengers, 214–15  
money and effort, 214  
ordinary passengers, 215  
security checkpoints, 217–18  
TT programs, 215–17
- RPM *see* Radiation Portal Monitors (RPM)
- rural evacuation *see also* evacuation  
actions, 367–8  
coastal communities, 363  
communication issues, 372  
emergency management plan tasks, 364–6  
employee issues, 373  
Hurricane Sandy coastal counties, 371–2  
inadequate finances, 373–4  
public transportation systems, 366–7  
Sacramento region evacuation, 368–70  
school bus systems, 364, 367  
survey, transportation agencies, 367  
transit system, 364–5  
2006 Nationwide Plan Review, 364
- Sacramento region emergency response  
case study  
bus service, 369  
evacuation  
action report (AAR), 370  
and mock drill exercise, 369–70  
Yuba–Sutter Transit, 369
- transit  
operation effectiveness, 370  
services and population density, 368, 368
- Sacramento Transportation Area Network (STARNET) system, 370
- SAFE Port Act *see* Security and Accountability for Every (SAFE) Port Act
- SAFE Port Reauthorization Act, 249
- SCADA *see* supervisory control and data acquisition (SCADA)
- Scanning Hydrographic Operational Airborne LIDAR Survey (SHOALS), 301
- scintillator-based detectors, 111–13

- seaport, scanning technology  
accuracy, 245  
European Union arguments, 248  
evaluation, 245  
high-risk scanning, 247  
integrated, 243  
100% scanning, 247, 249, 250  
portals, 241, 241, 242  
AT 580 Radiation Portal Monitor (RPM), 243  
SAFE Port Act, 249  
time, imaging cargo, 244
- seaports, security  
barriers  
  bioidentification, workers, 239  
  container inspection, 240  
  fences, road barricades, and gates, 239  
  patrol boat, 240, 240  
  vehicles and cargo containers, 240
- border and terror, 236–7  
capability/capacity, 235–6  
knowing and avoiding risk, 238–9  
Lawrence Livermore National Laboratory (LLNL) technology, 241
- portals  
  fixed security, 241, 241  
  movable security, 241, 242
- research  
  agenda, 252–3  
  high-risk methodology, 252  
  ideal scanning share, 251–2
- responsibility  
  federal commitment, 246–7  
  scanning *see* seaport, scanning technology
- technology  
  performance, 244–5  
  vendor, 242–4  
and terror, 234, 237
- search algorithms, 49, 50
- Secured Urban Transportation–European Demonstration (SECUR-ED), 160
- Secure Freight Initiative (SFI), 247
- Security and Accountability for Every (SAFE) Port Act, 246, 247
- security information management (SIM) system, 304
- security management and counterterrorism  
  comprehensive security plan, 197  
  containers, 198
- e-RAILSAFE program, 199
- Information Sharing and Cooperation (ISACs), 198  
network security systems, 199  
police patrols, 199  
recommendations, 200–201  
risk analysis, 198–9  
stakeholders, 201  
tank cars, 198  
U.S. Department of Homeland Security, 198
- security strategy  
cyberattack, 14  
data-mining activities, 14  
homeland security, 13–14  
prevention activities, 14  
protection, 15  
reasonable protection, 15  
regional jurisdictions, 14
- semiconductor detectors, 111–13
- SFI *see* Secure Freight Initiative (SFI)
- SHOALS *see* Scanning Hydrographic Operational Airborne LIDAR Survey (SHOALS)
- silent dispersion of radioactive material  
air activity concentrations, 140, 141  
air ventilation system, 138, 141  
casualties, 130–131  
CBRN training building, 137, 139  
floor surface deposition, spatial distribution, 140  
HEPA filters, 142  
radioactive concentration, air, 139  
RH program, 136, 139  
risk of individual exposure, 137
- SJTPO *see* South Jersey Transportation Planning Organization (SJTPO)
- skyjacking, 26
- Southeast Louisiana Catastrophic Hurricane Plan (SLHCP), 349
- South Jersey Transportation Planning Organization (SJTPO), 356
- Special Inspector General for Afghanistan Reconstruction (SIGAR), 75, 76
- Special Inspector General for Iraq Reconstruction (SIGIR), 75, 76
- STARNET system *see* Sacramento Transportation Area Network (STARNET) system
- State of Florida's Division of Emergency Management, 358

- Stay or Go policy, Australia, 320, 322  
ST-ISAC *see* Surface Transportation Information Sharing and Analysis Center (ST-ISAC)
- STSIs *see* surface transportation security inspectors (STSIs)
- Superfund Amendments and Reauthorization Act (SARA) Title III Act, 357
- supervisory control and data acquisition (SCADA), 66, 282, 288
- architecture, 81–2
- CI and homeland security budgets, 81
- cyberattacks, 82
- PPPs, 83
- surface transportation
- Israel, 3
- suicide attacks, 4
- Surface Transportation Information Sharing and Analysis Center (ST-ISAC), 199–200
- surface transportation security inspectors (STSIs)
- Congress and industry officials, 182
- GAO recommendations, 183, 185
- surveillance and communications
- technologies, 157–9
- terrorist attacks
- Islamic terrorism, 4
- maritime terrorism threat, 4
- public transportation, 3
- suicide attacks, 4
- suicide bombing, 3
- surface transportation, 3–4
- train bombing, 3
- terrorist targeting, public transport
- attacks, mass public transportation, 25
- collateral damage, 33
- criminalization, acts and statements, 33
- hijacking, 26–8
- hostage and murder, acts of, 25
- Islamic justification *see* mass transportation attacks, Islamic justification
- personal criminal culpability, principle of, 33
- training programs for security, 159–60
- transit security
- anticrime and antiterrorism efforts, 169–70
- coordination strategies, 161–3
- crime attractors, 168
- crime prevention, 169
- cybersecurity, 172
- description, 151–2
- environmental design, 163–8
- information and outreach campaigns, 160–161
- natural surveillance, 169–70
- open and public systems, 152
- physical attributes, 171
- policing, 156–7
- screening of passengers and luggage, 152
- surveillance and communications technologies, 157–9
- technologies, 152
- training programs, 159–60
- transit terrorism *see* transit terrorism
- transit terrorism
- bombings, 155
- characteristics, transportation, 152, 153
- crowds, 153–4
- definition, 154
- economic disruptions, 155
- failed plans, 155
- FBI's official definition, 154
- political volatility, 156
- rail and bus transit operators, 155
- stations, buses and trains, 152
- Transit Watch, 161
- transportation sector security
- homeland security
- CI systems, 70
- DHS's 18 CI sectors framework, 71, **71**
- DHS 7 US transportation system
- subsectors, 69–70, **70**
- transportation metasystem, 72
- natural disasters, 68–9
- 9/11 attacks, 69
- transportation-oriented attacks, 69
- Transportation Security Administration (TSA)
- Department of Homeland Security
- (DHS), 212
- federal agency, 181
- FEMA, 183, 184
- GAO recommendations, 183
- information sharing process, 184–5
- performance, 212–13
- rail security provisions, 182
- Senate bill, 222
- STSI program, 182–3

- Transportation Systems and Technology*, 38
- transportation, threats and challenges  
CI sector, 73  
demands, 72  
DHS budget trends, 74, 74  
federal bureaucratic reform, 73  
FY 2013 budget, 77, 78  
highway sector, 79–80  
Special Inspector General for Afghanistan Reconstruction (SIGAR), 75, **76**
- Special Inspector General for Iraq Reconstruction (SIGIR), 75, **76**
- supervisory control and data acquisition (SCADA), 81–3
- Transportation Worker Identification Credential (TWIC) program  
bureaucratic supply  
buffering, 266  
disqualifications, 263–4  
information asymmetry, 265  
marine terminal facilities, 263  
National Employment Law Project (2009), 263  
natural monopoly, 266  
security threat determinations, 263  
decentralization, 261–2  
description, 258  
goal, 258  
implementation, 258–9  
privatization  
government contracting, 260  
long-term contract, 260  
market failure, 261
- Traveler's perceptions and security  
methodological framework, 273  
decision-making behavior, individual, 273  
levels, 272
- port of Chios *see* port of Chios (case study)
- regulations, ports protection, 271
- security on port choice *see* port choice model
- terrorist attacks, 271
- trusted traveler (TT) programs *see also* transportation security administration (TSA)  
CAC director, 217  
national aviation security authorities, 215  
RAND Corporation, 216  
SWIFT system, 215
- TSA *see* Transportation Security Administration (TSA)
- TWIC program *see* Transportation Worker Identification Credential (TWIC) program
- unmanned ground vehicle (UGV), 60, 121, 122, 124
- US National Research Council, 38
- Victoria State Emergency Services (VICSES), 325
- video surveillance, 157–9, 168
- Washington Metropolitan Area Transit Authority (WMATA), 168
- weapons of mass destruction (WMD), 196, 198
- whistle-blowing activity, 161

# **WILEY END USER LICENSE AGREEMENT**

Go to [www.wiley.com/go/eula](http://www.wiley.com/go/eula) to access Wiley's ebook EULA.