Protecting the Nation's Seaports: Balancing Security and Cost

• • •

Editors:
Jon D. Haveman
Howard J. Shatz

2006

Library of Congress Cataloging-in-Publication Data
Protecting the nation's seaports: balancing security and cost / edited by Jon D. Haveman, Howard J. Shatz
p. cm.
Includes bibliographical references and indexes.
ISBN-13: 978-1-58213-120-7
ISBN-10: 1-58213-120-1
1. Harbors—Security measures—United States—Economic aspects. 2. Marine terminals—Security measures—United States—Economic aspects. 3. Shipping—Security measures—United States. 4. Terrorism—United States—Prevention—Economic aspects. I. Haveman, Jon D., 1964-II. Shatz, Howard J.
HE553.P76 2006
363.325'938710973—dc22
2006011932

Foreword

It is sometimes difficult to understand how much the world has changed since September 11. Even diplomats and foreign policy experts, who have far greater knowledge than most, have difficulty understanding all the consequences of events that have unfolded since September 11. One certain consequence is that the daily media reports of death and destruction from all over the world have made it imperative to intensify security measures in many ways.

With this report, *Protecting the Nation's Seaports: Balancing Security and Cost*, PPIC tries to shed some light on how one significant element of these global security imperatives is affecting Americans and Californians. California is home to three large seaports that are of major significance to the nation's economy—Los Angeles, Long Beach, and Oakland. The authors in this volume inform us that all California ports are vulnerable to a terrorist attack and that disabling any of the big three could have serious implications for the economic health of the region, as well as for lives and property in the immediate vicinity.

This volume is comprehensive—it describes and analyzes what could happen if a terrorist attack on a port were to occur, what can be done to deter such an attack, the characteristics of U.S. port security programs, what factors stand in the way of an adequate port security policy, and some alternative methods for financing that policy. Most important, this multiauthored volume is not alarmist—it is a thoughtful and balanced look at a major problem and its context: how the global economy has fostered huge increases in international trade and how terrorists could exploit the vulnerability of this massive global goods movement.

Protecting the Nation's Seaports may well become a standard reference volume for understanding the issue of port security for the nation and particularly for California. The authors describe the problems

and the solutions, but full implementation of new policy is still off in the future. Our hope is that this volume will help speed up the process of both policy development and implementation.

David W. Lyon
President and CEO
Public Policy Institute of California

Contents

Foreword iii
Figures xi
Tables xiii
Acknowledgments xv
Acronyms xix
Map of the Ports of Los Angeles and Long Beach xxiii

1. INTRODUCTION AND SUMMARY
by Jon D. Haveman and Howard J. Shatz 1
The Issue of Port Security 1
The PPIC Port Security Project 5
Summary of Main Findings 6
The Economic Effects of a Terrorist Attack on a Port 6
Best Practices in Port Security 11
Programs and Finance 16
Implications and Conclusions 23
References 28

2. PORTS, TRADE, AND TERRORISM: BALANCING THE CATASTROPHIC AND THE CHRONIC
by Edward E. Leamer and Christopher Thornberg 31
Introduction 31
The Cost-Benefit Analysis of Security 35
Most Shocks Do Not Cause Recessions 37
September 11 Did Not Cause the 2001 Recession 37
Natural Disasters Also Do Not Cause Recessions 39
How Much Disruption to Supply Chains? 42
The Problem Is With Labor 45
Previous Port Closures Hold Lessons for the Present 47
Previous Port Shutdowns Have Not Had a Great Effect on the Economy 51
Event Studies 56

Summary and Conclusions 59
Appendix 63
References 67

3. THE COSTS OF A TERRORIST ATTACK ON TERMINAL ISLAND AT THE TWIN PORTS OF LOS ANGELES AND LONG BEACH
by Peter Gordon, James E. Moore, II, Harry W. Richardson, and Qisheng Pan 71
Introduction 71
The Los Angeles and Long Beach Ports 73
The Southern California Planning Model 74
Radiological Bomb Attack Simulations 76
Terminal Island Attack Simulation 79
Qualifications and Comparisons 86
Conclusions 89
References 89

4. BOOM BOXES: CONTAINERS AND TERRORISM
by Stephen S. Cohen 91
Introduction 91
Threats 94
Direct Catastrophic Damage 94
Disabling Autoimmune Reactions 99
Itineraries, Scenarios, and Documentation: Or, One Container, Two Containers, Three Containers, Four . . . 100
Simple and Less-Simple Itineraries 101
Mixed Loads and Complicated Itineraries 103
"Container Bob" and Other Indicators 104
Defense 107
Layers 108
Conclusion 120
The Threats 120
The Constraints 120
The Approach to Defense 120
References 124

5. HARNESSING A TROJAN HORSE: ALIGNING SECURITY INVESTMENTS WITH COMMERCIAL TRAJECTORIES IN CARGO CONTAINER SHIPPING
by Jay Stowsky 129
Introduction 129
How Has the Private Sector Responded to the Terrorist Threat to Shipping and Ports? 132
The Coexistence of Successive Technology Generations 135
Other Factors Shaping the Private Sector Response 137
The Need for Standards 138
"Public Good" Aspects of Maritime and Port Security 139
Liability Issues 140
Tradeoffs Between Security and Other Societal Values 142
The Special Sensitivity of the Security Market to Terrorist Events 143
Key Technologies 143
Sensor Technologies 144
Identification and Authentication Technologies 145
Screening Technologies 146
Surveillance Technologies 147
Antitamper Seals and Tracking and Inspection Technologies 147
Integrated Solution and Data Analysis Technologies 149
Conclusions and Policy Recommendations 151
References 153

6. GOVERNANCE CHALLENGES IN PORT SECURITY: A CASE STUDY OF EMERGENCY RESPONSE CAPABILITIES AT THE PORTS OF LOS ANGELES AND LONG BEACH
by Amy B. Zegart, Matthew C. Hipp, and Seth K. Jacobson . . 155
Introduction 155
Organizational Challenges 157
Background 157
Findings and Recommendations 162
Status of Implementation 165
Conceptual Challenges 168
Background 168

Community Emergency Response Teams 171
Findings and Recommendations 172
Status of Implementation 173
Obstacles and Success Factors 176
Key Success Factors 178
Conclusion 180
Interviews 181
References 182

7. THE GOVERNMENT RESPONSE: U.S. PORT SECURITY PROGRAMS
by Jon D. Haveman, Howard J. Shatz, and Ernesto Vilchis . . . 185
Introduction 185
Port Security Before the September 11 Attacks 187
Current Port Security Measures 190
Maritime Transportation Security Act of 2002 191
The Container Security Initiative 197
The Customs Trade Partnership Against Terrorism 198
Other Customs and Border Protection Programs 201
Federal Port Security Grants 202
Evaluating Port Security Policies 207
Optimizing Security Programs, Resources, and Activities 208
Effectiveness 215
Unclear or Duplicated Authority and Lack of Priorities and Implementation 219
Funding 223
Conclusion 224
References 226

8. FINANCING PORT SECURITY
by Jon D. Haveman and Howard J. Shatz 233
Introduction 233
Efficiently Financing Port Security 236
Public Goods and Port Security 237
Negative Externalities and Port Activity 237
The Absence of Private Insurance Markets 241
Methods for Financing Port Security 245
Benefits and Costs 248

Implications for Financing Port Security 251
References 253

Glossary 257

About the Authors 265

Related PPIC Publications 271

Figures

2.1. Annual Number of Significant Terrorist Attacks on the United States, 1968–2003 32
2.2. Growth in Real GDP and Consumer Spending, 2000–2002 38
2.3. Indexes of Personal Income Around Significant Local Events 39
2.4. Indexes of Payroll Employment Around Disasters 41
2.5. U.S. Goods Trade and the 1960s Strikes 48
2.6. Imports Through California Customs Districts, 2002–2003 52
2.7. National Imports of Goods During Previous Port Shutdowns 53
2.8. Value of Manufacturing Production During Port Shutdowns 55
2.9. Producer Prices Around Past Labor-Related Shutdowns . . 56
2.10. Quarterly Changes in Real Consumer Spending on Goods 60
3.1. Spatial Distribution of Job Losses from a One-Year Closure of Terminal Island 84
7.1. Port Security Decision Structure 209

Tables

1.1. California Port Security Grant Program Allocations, Fiscal Year 2005 20
2.1. Value of Trade Through Los Angeles County Ports, 2003 43
2.2. Imports by Transport Type 49
2.3. Inventory-to-Sales Ratios 51
2.4. Employment Growth and Port Strikes 57
2.5. Port Shutdown Effect on Trade 58
2A.1. Economic Performance Regressions with Strike Control Dummy Variables 64
3.1a. Output and Employment Losses from a 15-Day Closure of the Ports of Los Angeles and Long Beach 78
3.1b. Output and Employment Losses from a 120-Day Closure of the Ports of Los Angeles and Long Beach 78
3.2. Change in Transportation Network Delay Costs for Multiple Impact Scenarios 80
3.3. Highway and Rail Access Bridges to Terminal Island 81
3.4. Output and Employment Losses from a One-Year Closure of Terminal Island 82
3.5. Total Output and Highway Network Losses for Alternative Bridge Reconstruction Periods 85
6.1. Agencies, and Their Political Jurisdictions, Responsible for Port Security at the Los Angeles/Long Beach Port Complex 159
7.1. Estimated Costs and Benefits of MTSA Measures 193
7.2. Foreign Ports Participating in the CSI 199
7.3. Federal Port Security Grants 203

Acknowledgments

A great many people proved instrumental to the completion of this project. Ellen Hanak and Mark Baldassare carefully read the manuscript at various stages, Richard Greene proved a thorough and helpful editor and mapmaker, and Joyce Peterson provided an additional review. External reviews of the entire manuscript by Michael Nacht, Jack Riley, and Margaret Wrightson, and of individual chapters by Randolph Hall, Jack Kyser, John Martin, Jon Sonstelie, and Page Stoutland, provided essential feedback and quality control. Any errors of fact or emphasis remain those of the editors or authors. Ernesto Vilchis, Greg Wright, and Ethan Jennings served as research associates (as well as a co-author in the case of Vilchis), and Wright took primary responsibility for preparing the list of acronyms and the glossary. Jennifer Paluch provided additional cartographic efforts and expertise. Patricia Bedrosian gave the manuscript a final polish.

Numerous port security experts took part in PPIC programs or otherwise discussed the issues with us, often candidly. The editors thank Michael Nacht, Steven Cash, Marc MacDonald, Gerald Swanson, and Lawrence Thibeaux for helping kick off the project at a public forum on port security, as well as Steve Flynn and Page Stoutland for giving separate presentations on port security. Others from the private sector, academia, and government participated in a private workshop at the beginning of the project and at a midterm update, helping keep the project on course. The editors also thank security experts at several of California's major ports, staff members of the U.S. Senate and House of Representatives, staff of the Transportation Security Administration, and Coast Guard officials in Los Angeles, Oakland, and Washington, D.C., for sharing their time and expertise. Thanks also go to participants at a symposium on Economic Costs and Consequences of a Terrorist Attack, University of Southern California Center for Risk and

Economic Analysis of Terrorism Events, for comments on an early draft of Chapter 7.

The authors of each chapter also acknowledge a number of people and organizations who contributed to their work at various stages.

For Chapter 2, Edward E. Leamer and Christopher Thornberg thank Jeany Zhao for research assistance and several security experts for helping them understand the types of risks that the ports of Los Angeles and Long Beach face.

The research for Chapter 3, by Peter Gordon, James E. Moore, II, Harry W. Richardson, and Qisheng Pan, was supported by the U.S. Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number N00014-05-0630. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the U.S. Department of Homeland Security.

Chapter 4, by Stephen S. Cohen, draws on ongoing research at the Berkeley Roundtable on the International Economy (BRIE) on port security and mobile communications supported, in part, by the European Union and DoCoMo Mobile Society Institute. Face-to-face interviews and extended conversations made this work possible. Many people contributed their time and patience in efforts to provide information on this complex and delicate subject. Not all wish to be acknowledged publicly. Sander Doves at the Port of Rotterdam, Steve Flynn at the Council on Foreign Relations, Howard Hall at Lawrence Livermore National Laboratory, Craig Epperson at the Pacific Maritime Association, Peter Wolters at the European Intermodal Association, Dietmar Jost at the World Customs Organization, Roland Van Bocket at the European Union, Der-Horug Lee in Singapore, Francesco Messineo and Antonio Barbara in Italy, and Admirals Dassatti and Scarlatti of the Italian Navy were generous with their time, knowledge, and good humor. Berkeley undergraduate Sara Karubian contributed to the research and to the maintenance of good spirits.

For Chapter 5, Jay Stowsky thanks John Gage and Linda Schacht-Gage for their generous gift to the Information Technology and Homeland Security Project at the Richard and Rhoda Goldman School

of Public Policy, University of California, Berkeley, which supported this work.

For Chapter 6, Amy B. Zegart, Matthew C. Hipp, and Seth K. Jacobson thank Richard Riordan, Peter Neffenger, Jack Weiss, Don Knabe, and Janice Hahn for their support of this project, as well as the 75 government officials, labor representatives, and shipping industry executives who generously shared their insights and expertise in personal interviews.

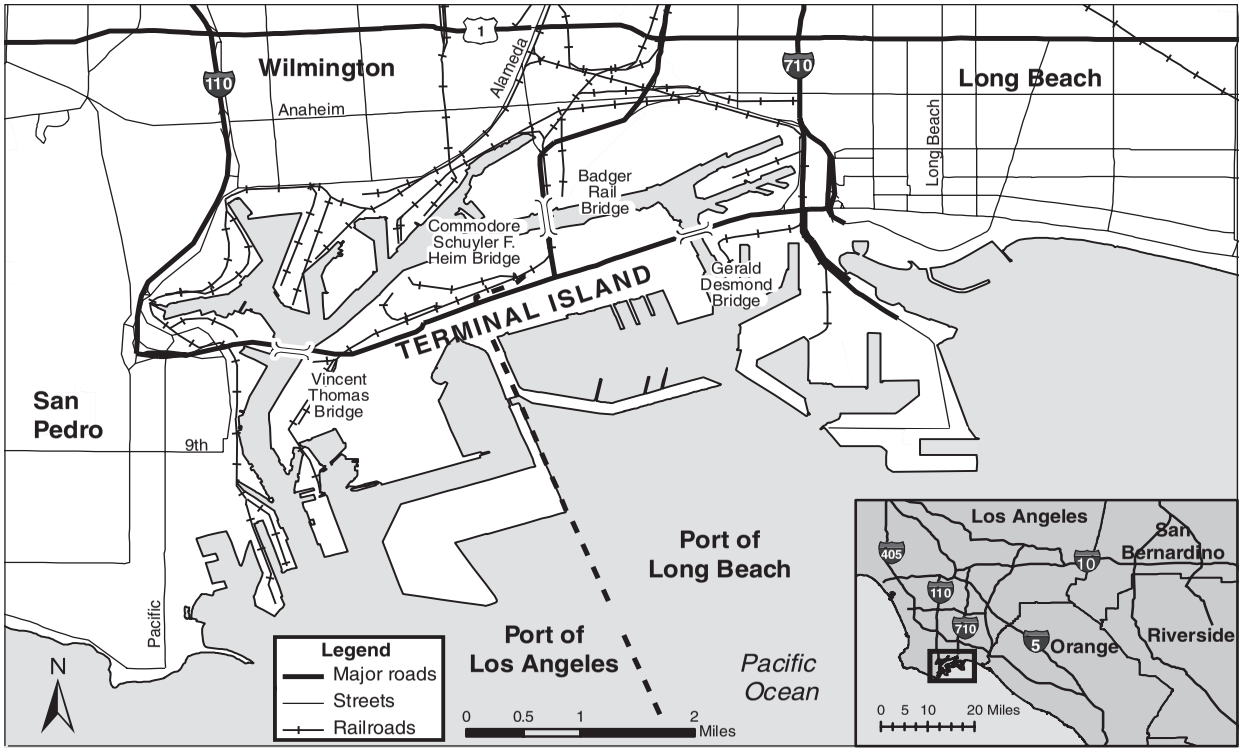
Finally, the editors thank the authors of Chapters 2, 3, 4, 5, and 6 for the overall quality of their work and their patience and good humor in dealing with reviews and numerous revisions.

Acronyms

AIS	Automatic Identification System
AMS	Area Maritime Security
BEA	Bureau of Economic Analysis
BRIE	Berkeley Roundtable on the International Economy
CBP	Customs and Border Protection
CBRN	Chemical, Biological, Radiological, and Nuclear Weapons
CEO	Chief Executive Officer
CERT	Community Emergency Response Team
CFS	Commodity Flow Survey
CMSA	Consolidated Metropolitan Statistical Area
CREATE	Center for Risk and Economic Analysis of Terrorism Events
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
DHS	Department of Homeland Security
DOT	Department of Transportation
EPA	Environmental Protection Agency
EU	European Union
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
G-7	Group of Seven
GAO	Government Accountability Office, formerly General Accounting Office
GDP	Gross Domestic Product
GPS	Global Positioning System
HSPD	Homeland Security Presidential Directive
ICS	Incident Command System
ICT	Institute for Counter-Terrorism

ILWU	International Longshore and Warehouse Union
IMO	International Maritime Organization
IMPLAN	Impact Analysis for Planning
IO	Input-Output
ISPS	International Ship and Port Facility Security
IT	Information Technology
LAX	Los Angeles International Airport
LLNL	Lawrence Livermore National Laboratory
MARAD	Maritime Administration
MARSEC	Maritime Security
MTS	Marine Transportation System
MTSA	Maritime Transportation Security Act
NOAA	National Oceanic and Atmospheric Administration
OCS	Outer Continental Shelf
ODP	Office of Domestic Preparedness
OECD	Organisation for Economic Cooperation and Development
OSC	Operation Safe Commerce
PCE	Passenger Car Equivalent
PMA	Pacific Maritime Association
PMSA	Primary Metropolitan Statistical Area
PPI	Producer Price Index
R&D	Research and Development
RDD	Radiological Dispersal Device
REM	Roentgen Equivalent Man
RFID	Radio Frequency Identification
RPM	Radiation Portal Monitor
SA	Seasonally Adjusted
SAAR	Seasonally Adjusted Annual Rate
SCAG	Southern California Association of Governments
SCPM	Southern California Planning Model
SHSP	State Homeland Security Program
SLGCP	State and Local Government Coordination and Preparedness
SOLAS	Safety of Life at Sea
TAZ	Traffic Analysis Zone

TEU	Twenty-Foot-Equivalent Unit
TIA	Terrorism Information Awareness, formerly Total Information Awareness
TMSARM	Transportation Security Administration Maritime Self-Assessment Risk Module
TRIA	Terrorism Risk Insurance Act
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
UASI	Urban Areas Security Initiative
UPC	Universal Product Code
USCG	United States Coast Guard
VAR	Vector Autoregression
VLSI	Very-Large-Scale Integrated
WMD	Weapons of Mass Destruction



The Ports of Los Angeles and Long Beach

1. Introduction and Summary

Jon D. Haveman and Howard J. Shatz
Public Policy Institute of California

Immediately following the terrorist attacks of September 11, 2001, the United States shut down its air traffic system for several days. In a less-well-known move, the government also temporarily halted the maritime transportation system, preventing ships approaching U.S. shores from reaching their destinations. Just as airplanes could serve as weapons, so could ships and their cargo. In the days, weeks, and months following the attacks, official and public attention focused much more intensely on increasing the safety of air travel than on securing the nation's seaports. However, seaport vulnerabilities did not go unnoticed. By late 2002, the U.S. Congress had passed legislation and government agencies had begun implementing programs directed at securing the nation's seaports. But are the port security policies, programs, and mechanisms now in place equal to the task, and what might be done to improve them? This report addresses those questions by considering the likely economic effects of a terrorist attack on a port, best practices in key areas of port security, how well government programs respond to major challenges in port security, and how port security should be financed.

The Issue of Port Security

The term "port security" serves as shorthand for the broad effort to secure the entire maritime supply chain, from the factory gate in a foreign country to the final destination of the product in the United States. The need to secure ports and the supply chain feeding goods into the ports stems from two concerns. The first is that transporting something from one place to another—the very activity that the ports facilitate—is an important activity for terrorists. Terrorists could use a

port as a conduit through which to build an arsenal within the nation's borders.

The second concern is that ports themselves present attractive targets for terrorists. Ports are a significant potential choke point for an enormous amount of economic activity. The 361 U.S. seaports make an immense contribution to U.S. trade and the U.S. economy. They move about 80 percent of all U.S. international trade by weight, and about 95 percent of all U.S. overseas trade, excluding trade with Mexico and Canada. By value, $807 billion worth of goods flowed through the seaports in 2003, about 41 percent of all U.S. international goods trade. This value is higher than the value of trade moved by all modes in any single leading industrial country except Germany. Temporarily shutting down a major U.S. port could impose significant economic costs throughout not only the United States but also the world. Al-Qaeda leader Osama bin Laden has labeled the destruction of the U.S. economy as one of his goals: "If their economy is finished, they will become too busy to enslave oppressed people. It is very important to concentrate on hitting the U.S. economy with every available means."[1]

The potential for a port closure to disrupt economic activity has been made clear several times in recent years. In 2002, the closure of all West Coast ports was clearly responsible for some element of economic disruption, with estimates of lost activity ranging from the hundreds of millions of dollars per day to several billion. In September 2005, Hurricane Katrina further served to reinforce the fact that ports are an integral feature of our goods distribution system. The closure of the Port of New Orleans and many smaller ports along the Gulf Coast is likely to have adversely affected U.S. grain exports, although at the time of this writing, cost estimates were not available. Hurricane Katrina further illustrated the effects of disruptions to the flow of oil, gasoline, and natural gas to the nation's economy. That a natural disaster can produce such a result implies that an attack on oil terminals at U.S. ports could be both desirable and effective for terrorists.

Beyond their economic role, the largest seaports are also near major population centers, so the use of a weapon of mass destruction at a port

---

[1]Agence France Presse (2001).

could injure or kill thousands of people. In addition, a weapon such as a nuclear device could cause vast environmental and social disruption and destroy important non-port infrastructure in these urban areas such as airports and highway networks.

How much risk is there for either of these concerns? U.S. law enforcement, academic, and business analysts believe that although the likelihood of an ocean container being used in a terrorist attack is low, the vulnerability of the maritime transportation system is extremely high, and the consequence of a security breach, such as the smuggling of a weapon of mass destruction into the country, would be disastrous.[2] Others take issue with the notion that the likelihood of a container attack is low, believing that an increase in global maritime terrorism in 2004 and the reputed appointment late that year of a maritime specialist as head of al-Qaeda in Saudi Arabia portended a significant maritime attack.[3]

Before September 11, maritime experts offered this broad definition of port security: "protective measures taken to prevent crime and maintain a state of freedom from danger, harm, or risk of loss to person or property."[4] This definition failed to include the dangers now understood to be part of the terrorism threat. An updated definition today might read, "protective measures taken to secure the maritime-related intermodal supply chain from terrorism, the unwitting transmission of terrorism-related assets, and crime; effective response should those measures fail; and freedom from danger, harm, and loss to person and property."

Port security is a challenge for many reasons. In the fall of 2000, security at America's ports was labeled as generally poor to fair.[5]

---

[2]U.S. Government Accountability Office (2005a), p. 7.

[3]According to Aegis Defense Services Ltd. (2004), Saud Hamud al-Utaibi, the al-Qaeda operative, was a maritime specialist linked to the 2000 attack on the USS *Cole* and the 2002 attack on the French supertanker M.V. *Limburg*. The appointment ultimately did not provide significant upside career potential, however, because Al-Utaibi reportedly was killed in a gun battle with Saudi security officials in April 2005 (CNN.com, 2005, and Aljazeera.net, 2005).

[4]Interagency Commission on Crime and Security in U.S. Seaports (2000).

[5]Interagency Commission on Crime and Security in U.S. Seaports (2000).

Immediately after the September 11 attacks, the greatest impediment to improving port security was, therefore, the extent to which it had previously been neglected. Although officials are no longer neglecting security, numerous factors make port security planning and implementation a continuing challenge. These include

- **Volume.** An extremely large amount of goods flows through the maritime supply chain. In 2004, America's ports handled almost 20 million ocean containers.[6]
- **Intermodality.** Goods arrive at and depart from the port not only by ship but by rail and truck.
- **Jurisdictional conflicts.** Federal, state, and local governments all may have oversight over some portion of port activities. In addition, some ports are managed by local or regional port authorities, whereas others are managed by local or state governments or by private entities.
- **Quantity of stakeholders.** Carriers, shippers, logistics firms, producers, labor unions, and others all work at or use the ports and all must be involved in security efforts for these to be effective.
- **Global nature of industry.** Any serious security effort requires international cooperation from foreign governments, foreign port operators, and foreign ship owners.
- **Time sensitivity.** Production has moved to just-in-time processes, with manufacturers relying on steady shipments of inputs.
- **Public and private involvement.** Both sectors are likely to be interested in having the other carry the burden of financing or even planning security efforts.

Port security has important implications for California. In terms of container volumes, the California ports of Los Angeles, Long Beach, and Oakland are the largest, second-largest, and fourth-largest ports in the United States. Combined, they handled 40 percent of all containers that flowed through U.S. ports in 2004. They handled 43.2 percent of

[6]American Association of Port Authorities (2005).

loaded import containers, which present the greatest threat.[7] In terms of the value of total trade, Los Angeles, Long Beach, and Oakland were ranked first, fifth, and 19th among all U.S. ports—air, land, and sea—in 2003, the most recent year of available data, handling 12.3 percent of all U.S. international trade.[8]

The PPIC Port Security Project

The purpose of this report is to explore the economics and governance of port security. The chapters add value to a growing policy conversation in three broad areas. The first, discussed in Chapters 2 and 3, covers the economic consequences of a terrorist attack on a port. Such an analysis can shed light on the relative importance of protecting ports as opposed to other assets, such as skyscrapers, shopping malls, railroads, or airports. Estimates of how much a successful attack might cost the U.S. economy have ranged in the billions and even trillions of dollars, depending on the nature of the attack. Better defining the possible costs of a terrorist attack on a port can help policymakers better allocate scarce security resources, including money, people, and equipment.

The U.S. Government Accountability Office (GAO), the federal government's chief fiscal and program watchdog, recommends that the United States allocate its security resources using a risk management approach.[9] This includes assessments of threat (the likelihood of terrorist activity against an asset), vulnerability (the asset's weaknesses), and criticality (the relative importance of the asset). Shortly after taking over as head of the Department of Homeland Security (DHS) in early 2005, Michael Chertoff emphasized the use of a risk-management strategy for the department.[10] Although this approach may be best, implementation will not be easy because each element is difficult to quantify.

---

[7]These proportions are in terms of twenty-foot equivalent container units (TEUs), the standard measure of container traffic (American Association of Port Authorities, 2005).

[8]U.S. Department of Transportation (2004).

[9]Decker (2001).

[10]Chertoff (2005a, 2005b).

The second broad area, discussed in Chapters 4, 5, and 6, covers best practices in key areas of port security. These include the question of how to seal the container supply chain, how to get the most out of billions of dollars worth of technology development, and how to prepare for emergency response in the case of a terrorist incident at a port.

The third broad area, discussed in Chapters 7 and 8, assesses the government response to the challenges raised in the economics and best practices chapters. How well do government programs respond to the key challenges of port security? How can these programs be improved? The final chapter in this study explores an issue that has stumped government and business since the beginning of new efforts at port security: raising the finances to pay for initiatives, staff, and programs that policymakers view as necessary to an effective port security venture.

Summary of Main Findings

The Economic Effects of a Terrorist Attack on a Port

The ports of Los Angeles and Long Beach are jurisdictionally separate but share San Pedro Bay and effectively serve as one giant port complex (see the port map, p. xxiii). Combined, the complex is the largest port by value in the United States and the fifth-largest container port in the world. If terrorists wanted to wreak havoc on the U.S. economy, the Los Angeles–Long Beach complex would certainly be a prime target for attack. In 2004, the complex processed $243 billion worth of traded goods, just over 10 percent of all U.S. trade, 25 percent of all waterborne trade, or an amount equal to about 2 percent of U.S. gross domestic product (GDP). Because imports constitute the vast majority of this trade, and because these imports are often used as inputs to other products, a terrorist attack on these ports could disrupt the U.S. economy. Opinions on the extent of disruption differ significantly, however.

In Chapter 2, Edward E. Leamer and Christopher Thornberg argue that the actual costs of an attack on the Los Angeles–Long Beach port complex may not be as high as many fear. For example, if a port is closed, many shippers will reroute their shipments through other ports. In addition, displaced workers will seek alternative employment. As a

result, the economy will adjust. Some output will be lost, but it may be so small in magnitude that it will not reveal itself in data that track national or even regional macroeconomic trends.

The authors provide examples of other disruptions that might have caused severe economic damage but did not, such as the terrorist attacks of September 11, 2001. Consumer spending fell immediately after the attacks but then rebounded sharply at the end of 2001, growing at an unprecedented, seasonally adjusted annual rate of 7 percent. Likewise, although retail sales fell immediately after the attacks, they returned to trend in November, only two months later. Some sectors did suffer, most notably the airline industry, which had already been in deep trouble before the end of the technology boom in early 2001. But consumer spending actually increased, suggesting that people reallocated the money that they would have spent on airline travel to other forms of consumption. Similarly, the authors argue that other disruptions such as hurricanes, earthquakes, and even labor disputes at seaports did have immediate negative economic effects but that these effects dissipated quickly as the economy adjusted. The message in this is that most such disruptions lead to business being delayed rather than business being cancelled, which in turn results in much less economic harm than would be expected.

In Chapter 3, Peter Gordon, James E. Moore, II, Harry W. Richardson, and Qisheng Pan provide a quite different analysis, suggesting that an attack on the port complex could have severe economic consequences. About 55 percent of the twin ports' trade goes through Terminal Island, which is connected to the mainland by three highway bridges and a rail bridge. One possible terrorism scenario is the successful destruction of all four of those bridges by conventional bombs, perhaps in a simultaneous attack of the type that al-Qaeda has become known for.[11] The economic effects depend on reconstruction time, and

---

[11]Simultaneous attacks attributed to al-Qaeda or its affiliates include the bombings of U.S. embassies in Kenya and Tanzania on August 7, 1998; the hijacking of four airplanes and the crashing of three of them into the World Trade Center in New York and the Pentagon in Washington, D.C., on September 11, 2001; the bombings of trains in Madrid on March 11, 2004; and the bombings in the London public transit system on July 7, 2005.

estimates of these effects are derived for reconstruction times ranging between three months and two years. Costs would rise as the disruption lengthened.

In the scenario of a one-year reconstruction, the U.S. economy could suffer losses of almost $45 billion, the authors argue. These include direct costs, indirect costs, and induced costs. Direct costs arise as a direct result of the halt in shipping. For example, if car parts are being imported, the car manufacturer can neither assemble nor sell more cars. Indirect costs result from the fact that other domestic firms supply parts to the same car manufacturer. These parts would no longer be needed, so these firms would sell fewer parts as an indirect result of the halt in trade. Induced costs result from the reduction of consumption spending by households whose members worked in the affected industries. About 64 percent of this loss would occur outside the five-county Los Angeles region; some would occur elsewhere in California, but most would occur outside the state.

These are not trivial costs. For comparison, the new eastern span of the San Francisco–Oakland Bay Bridge is expected to cost around $6 billion, and policymakers have gone to enormous pains finding money to pay for it. The estimated costs of a one-year closure of Terminal Island are more than seven times that large. Nevertheless, U.S. GDP is more than $11.7 trillion, next to which the economic costs of an attack do seem small.[12]

Such an attack would also cost jobs. Under the one-year scenario, the equivalent of 280,000 jobs would be lost before the ports were restored. Of these, 101,000 would be in the five-county Los Angeles region. If these jobs had been lost in 2004, and all the workers who occupied them remained in the labor force, the five-county unemployment rate could have been as high as 7.1 percent rather than the actual 5.9 percent. All of these costs likely would be magnified if

---

[12]For further comparison, the economic costs of the terrorist attacks on September 11, 2001, have been estimated at $83 billion for the New York City area economy by the New York City Partnership and Chamber of Commerce, $191 billion for the metropolitan areas throughout the nation by the Milken Institute, and other amounts by other groups (U.S. Government Accountability Office, 2002).

terrorists struck successfully at multiple ports, although the authors do not investigate this further possibility.

These two studies of economic effects serve as bookends to the question of the economic consequences of a terrorist attack at a port. We cannot say for certain whether the actual cost will be closer to $45 billion for a one-year closure of Terminal Island or something much less, in part because of the very different methods used in the two analyses. Although their methods differ, both are part of standard practice in the analysis of economic effects. The $45 billion figure in Chapter 3 results from a sophisticated computer analysis that examines the ripple effects of the port closures. This ripple effect occurs because in many cases imports are intermediate inputs to the production of some other good. As an example, should the disrupted trade include automobile parts, production at the automobile plant is slowed, reducing economic output. This methodology calculates economic costs as the sum total of economic activity disrupted because of the closure of the ports.

The more sanguine estimate of the economic effects, in Chapter 2, results from an evaluation of the observed economic disruption from previous similar events. This more direct examination of the economic evidence indicates that in many cases, particularly port closures of relatively short duration, economic activity is more delayed than disrupted. The authors find that consumers and producers wait out the strike, storm, or other disruption, all the while accumulating demand that occurs in a flurry once the flow of goods resumes. The evidence indicates that for longer disruptions, economic agents are very creative and can find ways to work around a bottleneck such as a closed port.

Reconciling these two views is extremely complex. Although it is tempting to embrace wholly one or the other of the estimates, there is merit in giving credence to each. In particular, their use as upper and lower bounds of the possible effects is beneficial. Surely the truth lies somewhere between a complete loss of economic activity and an economy that will work around it or make up for it later. There will surely be some delay and diversion of activity as opposed to its outright elimination, but just how much depends on the length of the closure and the availability of excess capacity at other ports. Unfortunately, evidence on either of these parameters is difficult to come by.

At the same time that these studies provide bookends, having a reasonable upper bound on the damages is helpful for policy planning and for carrying out the benefit-cost analysis necessary to efficiently implement port security policies. Other published estimates suggest that the cost of port-related terrorism could be as high as $1 trillion.[13] However, given the speculative nature of these other figures, they are much less useful for the development of appropriate policy responses to the terrorist threat.

Despite the differences in approach to the issue, both sets of authors agree on two points that hold valuable policy lessons. First, during the closure of all the ports on the West Coast in 2002, popular belief held that the closure was costing the U.S. economy $2 billion each day. A simple extrapolation leads to an annual cost of $730 billion, or about 6 percent of U.S. gross domestic product. Both analyses in this section find that such numbers exaggerate the scope of the problem.

Second, and more important, both sets of authors argue that costs can be minimized through effective preparation. In the specific case of Terminal Island, costs will depend on the duration of the interruption from the bridge attacks, and that duration will in turn depend on how quickly service can be restored—suggesting that contingency planning for a Long Beach–Los Angeles terrorist attack should have high priority.

More generally, a port attack scenario also calls for policy planning to ensure that any disruptions will be short. Firms engaged in international trade may need to keep higher inventories and should have their own contingency plans. To get commerce moving again in the aftermath of a port attack, the government should have a way to sort safe cargo from higher-risk cargo. Furthermore, an allocation arrangement—a market-based bidding system, for example—can be devised in advance to help prioritize cargo that will have built up offshore in the aftermath of an attack. These measures, and surely others, should prove useful in offsetting the overall economic costs of a significant terrorism-related

---

[13]O'Hanlon et al. (2003). Their most costly scenario involves weapons of mass destruction shipped via containers or the mail and causing extended shutdown of deliveries, physical destruction, contamination, massive loss of life, and medical costs.

port closure and reflect best practices that are the focus of the next three chapters of this report.

Best Practices in Port Security

These chapters reveal the need to consider several additional measures for port security. First is to ensure that port workers and emergency services workers are fully prepared for effective response. The next is to avoid panicked reactions on the part of both government and the population, which would turn a bad situation into a worse one. Chapters 4, 5, and 6 discuss the importance of these and other measures for container security, for security technology, and for governance issues in emergency response, respectively.

In Chapter 4, Stephen S. Cohen considers the security threat that the container creates for the maritime transportation system. Each day, tens of thousands of containers flow through U.S. ports, largely undisturbed in their trip from one part of the world to another. In general, containers are loaded and sealed, or perhaps only closed and not sealed, well inland of a port. They are then transferred by truck, or truck and train, to a seaport, where they are loaded onto a ship. Following the sea journey, they are transferred to another truck, and perhaps another train, for a further journey over land to the ultimate destination.

Each container trip to the United States has, on average, 17 different stops, or points at which the container's journey temporarily halts.[14] The adage "goods at rest are goods at risk" readily applies to the terrorist threat. The container will be at rest at any point in the journey that involves a change in mode of transportation. While at rest, the container is vulnerable to thieves and terrorists alike. Providing port security therefore involves closely scrutinizing activities not only at the port but at points all along the shipping chain. The truck driver picking up the container at the U.S. port, often poorly paid and possibly an illegal immigrant not well integrated into U.S. society, may himself represent a vulnerability in the system.

The issue is not merely that something could be put in a container illicitly for an attack on the port where it is unloaded but that nuclear

---

[14] Flynn (2004), p. 89.

weapons or radiological material could be inserted, shipped to the United States, moved inland without inspection, and then unloaded into the hands of terrorists. These objects could then be transported for use in major population centers—perhaps better targets than a port complex. Likewise, explosive material could be put in several containers and then detonated at or near port complexes around the same time, leading to a security reaction that could shut down the entire maritime transportation system until officials, and port workers and management, were certain the threat had passed.

There is no way to completely inspect all of the millions of containers entering the United States. They are about as large as a full-size moving van and are often tightly packed. Inspecting each thoroughly would bring commerce to a halt, exactly the kind of reaction that terrorists hope to generate.

Given the difficulties of complete inspection, defense needs to be layered, with checks at multiple stages on a container's journey. Even if a check at one stage has a low probability of uncovering a problem, multiple checks throughout the supply chain raise that probability a great deal. Such a layered defense can be divided into five areas: (1) intelligence—gaining information about which containers might be risky, (2) information about contents—having shippers notify authorities about the goods they are shipping, (3) procedural uniformity—creating standard procedures regarding packing and moving goods so that anomalies will be seen more easily, (4) limiting access—enforcing greater control over who may come near containers and ports, and (5) technology—the development of new inspection and tracking technologies.

None of these layers can be created in such a way that they work perfectly, but they might be able to work well enough. For instance, intelligence can be invaluable, but it fails to capture all valuable information all the time. More complete information will depend on the ability and willingness of shippers and ocean carriers to provide that information. Procedural uniformity will require the cooperation—happily or not—of tens of thousands of businesses involved in international maritime trade. Access limitations, especially to warehouse yards and shipping points overseas, could favor a few large businesses and

produce significant industry concentration, hurting less-powerful businesses and even entire countries. Advanced technologies can prove very effective, but they can also prove costly and may not operate as expected. Most especially, they may produce too many "false positives"—alarms indicating that something dangerous may be in the container when in fact it is benign. Physical inspection is then still necessary, leading to a slowdown in the system. With too many false positives, security officials start to ignore alarms until they miss a real positive—and a terrorist plan succeeds.

In Chapter 5, Jay Stowsky discusses how the need for more security and the promise of what advanced technologies can provide has led to the active development of security technology since the September 11 attacks. Companies are developing an array of new technologies, including sensor technologies, identification and authentication technologies, screening technologies, surveillance technologies, antitamper technologies, and tracking and inspection technologies.

Purchasers are now faced with deciding among three generations of technologies—those products that were just coming to market in late 2001, new products that integrate many of the tasks of the first-generation technologies, and products now under development in national laboratories or private companies. With this multiplicity of choices—types of products and generations of products—a new market in end-to-end security provision is developing.

The overriding policy issue related to technology adoption is whether the United States can achieve economic gains as well as security from these technologies. Cold War technology development is often portrayed as an example of defense expenditures creating beneficial economic effects through technology transfer from military to civilian uses. In reality, Stowsky contends, the economic benefits have been exaggerated and these expenditures sometimes merely distorted the country's economic and technological development with only negligible effects on security.

In the current wave of security technology development, the government can encourage beneficial effects by supporting, as much as possible, basic research and exploratory development, much as it did during the Cold War. This will attract more researchers from

universities and businesses, especially if they can retain the rights to the intellectual property they develop. Government can adopt policies that encourage its own agencies to buy commercial technology and modify it for security purposes, rather than developing new technology specifically for security purposes. The security modifications can remain secret, but the expanded market for open, commercial technologies can encourage more research and development. More than ever, technology development is an international venture. Government can also rethink and reform export and publication controls so that collaborations with foreign researchers become easier. Cutting off U.S. technology development from the world could lead to less-promising technologies, as well as to technologies that do not respond to international needs, in turn allowing foreign competitors to outpace U.S. companies in global markets.

Finally, government can focus its development efforts on those technologies that commercial sources are least likely to develop. Private businesses are keen to adopt and use tracking technology so that they know where goods are and whether they are being pilfered. However, private businesses are not so interested in producing technology that will detect threats to the entire maritime system or to the economy as a whole, that will help the entire supply chain operate through a terrorist attack, or that will allow it to be reconstituted quickly—the benefits are too diffuse for any single business to profit from them. However, the benefits are large for society, suggesting that government should pay special attention to technologies such as those that can remotely sense the presence of chemical, biological, radiological, and nuclear agents.

Even if layered container security and efficient technology development are implemented, there is still a possibility of a terrorist attack. No security system is impregnable. In the case of an attack, rapid, effective response has the potential to stave off much of the ensuing disruption. Moreover, effective emergency response to terrorist incidents is not just about humanitarian relief. It is also a vital factor in limiting economic damage. If port workers are injured or are unsure about their safety, they will leave the port, bringing work and commerce to a standstill. The effects of such uncertainty can ripple to other ports; the International Longshore and Warehouse Union motto—that an

injury to one is an injury to all—suggests that dockworkers will not readily go back to work at other ports if they see that their union brothers are being neglected in the wake of a terrorist event.

In Chapter 6, Amy B. Zegart, Matthew C. Hipp, and Seth K. Jacobson provide a case study of emergency response organization at the port complex of Los Angeles and Long Beach, describing some of the governance difficulties of effective response and some possible solutions. The vast and complex geographic area of the port facility is spread over two cities, and emergency response involves several different police and fire agencies. Two significant governance barriers to emergency response emerge. The first is organizational. Responsibility for port security falls to 15 different federal, state, and local agencies, with no one completely in charge. The second is conceptual. The emergency response template is for natural disasters, in which it was assumed that emergency responders would easily be able to reach the port complex. However, in the wake of a terrorist event, the risk of mass panic or other problems suggest that the port could be isolated during the initial period when response is most needed.

Fortunately, there are possible solutions. Inclusion of representatives from key agencies on a security committee can provide for coordination. Mandatory semi-annual meetings of top policymakers (the mayors of Los Angeles and Long Beach, city council members from the two cities whose jurisdictions include the ports, and the Los Angeles County supervisor whose jurisdiction includes the ports) could help make sure that safety and security recommendations are implemented. Port workers could be trained in basic emergency response so that in the event of an emergency, when the designated Los Angeles or Long Beach city responders are stuck on clogged highways, the workers themselves could be saving lives.

But even these seemingly simple measures are fraught with challenges. Representatives from key agencies in fact now gather at regular intervals as the Area Maritime Security Committee. However, no one has authority to force others to act—coordination depends on leadership and persuasion. Top elected officials responded by attempting to institutionalize high-level meetings but in fact representatives have apparently met only twice—once at a formal meeting in 2003 and once

at a security briefing and press conference that Senator Dianne Feinstein organized in early 2005. The emergency training for dockworkers proceeded more slowly than hoped. A shortage of qualified trainers, failure to establish an interagency joint training team, and lack of funding all stood in the way of speedier implementation.

What leads to success in overcoming governance obstacles? Not the importance of an issue—in the case of the ports of Los Angeles and Long Beach, even when everyone agreed on the importance of port security and a course of action, implementation would have failed without three success factors. First, there is no substitute for political leadership. The emergency training for dockworkers, for example, would have lagged even more than it did if former Los Angeles Mayor James Hahn had not taken responsibility for seeing that it moved forward. Second, neutral analysis of the governance issues can help, so that agencies and officials do not think that they are being called on to take action just to serve someone's political or commercial interest. Finally, long-term involvement can drive the parties to solutions. The authors have been working with the ports since 2003 and have found that success requires person-to-person diplomacy and the building of strong relationships.

Programs and Finance

Emergency response is one area of many that government has been called on to implement. In Chapter 7, Jon D. Haveman, Howard J. Shatz, and Ernesto Vilchis review how, in the wake of the September 11 attacks, the federal government moved quickly to address the vulnerability of U.S. ports. Different agencies started implementing new rules and experimenting with new programs, and on November 25, 2002, President George W. Bush signed the Maritime Transportation Security Act of 2002 (MTSA).

It was possible to produce this legislation quickly only because much of the legwork had already begun before the September 11 attacks, although most had focused on security against crime rather than against terrorism. Early efforts included a Department of Transportation port security planning guide in 1997, the establishment of the Marine Transportation System (MTS) Initiative in 1998, and the congressionally created MTS Task Force later that year. The Task Force's report, issued

in September 1999, recognized that rogue states and transnational terrorists could target U.S. critical infrastructure, including seaports, and made a number of recommendations regarding port security.[15]

In April 1999, reinforcing the efforts of Congress, President Bill Clinton established a commission to study crime in U.S. seaports and to examine the potential threats posed by terrorists and others to the people and critical infrastructures of seaport cities. At the time, the Federal Bureau of Investigation (FBI) considered the threat of terrorism directed at U.S. seaports to be low but also considered their vulnerability to be high; and the commission expressed the belief that an attack had the potential to cause significant damage.

Among the post–September 11 U.S. policy measures currently in place, four stand out: the MTSA, the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT), and a port security grant program run by the Department of Homeland Security. MTSA, led by the U.S. Coast Guard, calls for national, area, port facility, and vessel security plans that include ways to prevent terrorist incidents and respond to them. It also calls for new identity cards for transportation workers, new Coast Guard rapid-response teams, and other measures.

The Container Security Initiative, under the jurisdiction of U.S. Customs and Border Protection, effectively pushes U.S. borders outward by providing for advance screening and potential inspection of containers at foreign ports, before they arrive in the United States. The C-TPAT, also a U.S. Customs and Border Protection program, aims at getting companies involved in goods movement to seal their supply chains. Companies in the program include importers, logistics specialists, freight forwarders, and others connected with international trade. Those companies whose supply chains meet the requirements get fewer inspections at U.S. borders, freeing up customs officials to focus on riskier cargo.

Implementing MTSA in particular places a large financial burden on ports and the companies that operate port facilities. The grants program is designed to alleviate this burden by providing for federal government

---

[15]Marine Transportation System Task Force (1999).

contributions to private expenditures. It is one way the government recognized that methods of business and security had to change following September 11.

The authors evaluate port security policies, organizing concerns into four areas. The first of these is whether policies optimize security programs, resources, and activities: Are the measures instituted appropriate, in the sense of getting the most security for their cost and directing security assets optimally? The second is the effectiveness of programs. If complied with fully, will the plans and programs improve security? Will they be complied with? Third is the issue of unclear authority and priorities. In the sprint to create security measures, a number of laws covering the same issues were passed but not necessarily coordinated; and agencies were tasked with quickly obeying legislative mandates. Last is the issue of financing. Who is meant to pay for this? In some cases, these four issues are related.

One key optimizing issue involves the choice between prevention and recovery. Most port security efforts after September 11 aimed to prevent a terrorist incident from disrupting the maritime transportation system, with less attention paid to equally critical questions such as emergency response and system reconstitution. Other issues involved the inclusion of labor in port security planning and the balance between East Coast, Gulf Coast, and West Coast ports. Dockworkers have proven to be able eyes and ears at the terminals where ships dock and cargo is moved. Yet, in some cases, they were initially excluded from port security planning committees. Even now, tensions remain over the issue of creating secure identification cards for dockworkers, truckers, and other port workers who may have checkered backgrounds, and even criminal records, but who do not pose a terrorist threat. Additionally, it is not clear that federal programs are striking the right balance between different regions of the country. Of the three major container port areas—Los Angeles–Long Beach, New York–New Jersey, and Seattle-Tacoma—two are on the West Coast. Whether the West Coast ports have been given security assets proportional to their importance and the threat they face is under debate by policymakers.

The regional inconsistency arises in the case of the allocation of port security grants. In 2003, California ports handled 36 percent of all U.S.

waterborne imports and 49 percent of all waterborne containerized imports by value. They handled a much smaller proportion of the weight of national imports (11%) but more than 40 percent of containerized imports by weight. Despite the proportion of trade they handle, California ports and others in the maritime industry had received only 19 percent of all federal port-security-related grant money by late 2005. This apparent misallocation is similar to the more general allocation of homeland security funding, with federal formulas built in that have favored small states and eschew risk-based measures.[16]

This has started to change at the federal level. DHS used risk-based measures to select 35 areas as eligible for its fiscal year 2006 Urban Areas Security Initiative grants, one of several types of homeland security grants the department dispenses. At a press conference announcing the grant competition, DHS Secretary Chertoff said that the department would continue to design programs based on risk, as opposed to fixed formulas, whenever the law allowed and would continue to advocate a risk-based approach to programs.[17]

Lest state officials become indignant about grant formulas that favor small geographic areas, California does exactly the same thing with the homeland security money given to it by the federal government. In its allocation of $67.7 million of State Homeland Security Program grant money to counties in fiscal year 2005, California used a formula in which it gave $100,000 to each county and then an additional $1.71 per person to each county, resulting in actual allocations of $79.84 per person to sparsely populated Alpine County, $30.12 per person to Sierra County, $12.08 per person to Modoc County, and only $1.72 per person to Los Angeles County. The state used the same type of formula with $20.6 million in Law Enforcement Terrorism Prevention Program grants ($50,000 per county and then 49 cents per person per county), and $6.2 million in Emergency Management Performance grants ($40,000 per county and 11 cents per person per county). Absent was any recognition that threat, vulnerability, and criticality—the

---

[16]Ransdell (2004).

[17]U.S. Department of Homeland Security (2006).

cornerstones of a risk-based security allocation system—might not be correlated strongly with population, either positively or negatively.[18]

California's allocation of fiscal year 2005 port security grant program funds does allocate larger amounts to larger ports. California ports that received more waterborne imports in 2003 tended to get more money from the state's 2005 port security grant program, which is in turn funded with an allocation from the federal government. Considering the tremendous disparity in port sizes, the grants are fairly even. It is again not clear to what extent the state took account of threat, vulnerability, and criticality, as opposed to making sure that every port got something (Table 1.1).

The effectiveness of port security programs depends on two factors—whether they will be complied with and, even if fully complied

Table 1.1

California Port Security Grant Program Allocations, Fiscal Year 2005

Port	Imports ($ millions)	Import Share (%)	Grant Amount ($)	Grant Share (%)
Port of Los Angeles	105,875	38.7	750,000	15.2
Port of Long Beach	77,935	28.5	750,000	15.2
Port of Oakland	17,386	6.4	750,000	15.2
Port of Hueneme	5,184	1.9	450,000	9.1
Port of San Diego	4,463	1.6	750,000	15.2
Port of Richmond	1,932	0.7	450,000	9.1
Port of San Francisco	225	0.1	450,000	9.1
Port of Stockton	122	0.0	150,000	3.0
Port of Sacramento	70	0.0	150,000	3.0
Humboldt Bay Harbor District	25	0.0	15,000	3.0
Port of Redwood City	17	0.0	150,000	3.0
California total	273,398		4,950,000	

SOURCES: Office of Homeland Security (2005); U.S. Army Corps of Engineers (2005).

NOTES: Import values are from 2003. Not all California ports are listed. Accordingly, the first column does not sum to the California total. Other columns may not sum to totals because of rounding.

[18]Office of Homeland Security, Governor's Office of Emergency Services, and California Service Corps (2005).

with, whether they will improve security. Compliance is the weaker link. The Customs-Trade Partnership Against Terrorism, for example, depends on U.S. Customs and Border Protection validation of security plans for thousands of companies. However, given a lack of enforcement mechanisms, there is no guarantee that firms, once validated, will continue to carry out their security plans and procedures. Likewise, the Container Security Initiative depends on the cooperation of foreign governments. In some cases, foreign governments decline to inspect containers that U.S. authorities deem high-risk. The United States can then order the containers not to be loaded onto the ship at the foreign port or can inspect the container in its U.S. port of arrival. However, even with these options, some high-risk containers go uninspected (U.S. Government Accountability Office, 2005b).

Even full compliance will not guarantee success. As part of the Container Security Initiative, oceangoing ship operators must provide the manifest, or list of the contents of ship cargo, to U.S. officials in advance. However, the carrier has no way of knowing the accuracy of the manifest, since it gets the information from the individual companies shipping the goods.

The third issue, unclear authority and priorities, reflects in part the sprint to create new security measures. Laws covering the same issues were passed but not necessarily coordinated, and agencies were tasked with quickly obeying multiple legislative mandates. Two laws cover the grants program, and at least two laws cover worker identification cards. Agencies have worked out which set of requirements to follow. However, this does not necessarily mean that the will of Congress and the president is being followed because that will is unclear.

These new measures also failed to signal priorities and, as a result, the implementation of some initiatives is lagging. Examples include the transportation worker identification cards; development of a program to evaluate and secure systems of international intermodal transportation; and new investments in Coast Guard ships, helicopters, and airplanes in a program known as the Integrated Deepwater System.

In the final chapter of the volume, Jon D. Haveman and Howard J. Shatz consider the issue of financing. Who is to pay for port security? The federal grants program certainly will not cover the total cost of

implementing security measures. The U.S. Coast Guard estimated the cost of MTSA compliance to be $7.3 billion over a 10-year period. As of September 2005, the federal government had provided about $780 million. However, it is not necessary for the government to pay all the costs. The test is whether requirements are being fulfilled and whether private firms have the ability, not just the willingness, to cover a large share of the costs without serious disruption to economic activity. This financing puzzle remains an important unresolved issue in the economics and governance of port security. At its core, it is a question of who should bear responsibility for port security.

Absent political considerations, a solid case may be made that both government and business should pay some part, although finding the proper division is more difficult. In some ways, port security is like national defense, in that creating increased safety through security measures necessarily creates increased safety for everyone in the country. This suggests a strong role for federal government financing. However, the use of cargo containers by shippers causes danger to people in the vicinity of containers, while a gain accrues to shippers. Under this argument, they should pay for the increased danger their activities cause, and so this suggests private provision of port security finance. Finally, much of the risk can be shared through insurance and reinsurance markets, but terrorism insurance does not cover many types of terrorism threats, and many potential buyers have not actually purchased terrorism insurance. This suggests a role for government in helping create a functioning terrorism insurance market.

A variety of officials have advanced different plans for how the federal government can provide its share of port security financing. These include user fees, the diversion of customs revenues, and general revenues. In addition, California is contemplating the establishment of its own port security grant program with its own money rather than with federal money it receives—although this state-level program at best could serve as an adjunct rather than primary method of finance.

User fees, a possible solution, also have significant downsides. They could result in diversion of ship traffic to ports in other countries, Mexico and Canada in particular, or to other transportation modes, such as air cargo. Furthermore, their use would remove the burden from

society as a whole. The use of customs duties, although supported by many port officials, would create a pro-tariff lobby, when for more than 60 years, legislators from both major political parties have generally sought to reduce U.S. tariffs. Using customs duties for this new purpose would also mean cuts in the programs currently funded by customs duties. Additionally, ports have no claim on these duties—duties are taxes on imported goods, not taxes for using the ports. To say that a port has a claim on duties collected by virtue of its throughput is equivalent to saying that a retailer has a claim on the sales taxes collected through its business activities.

These conflicts suggest that the most economically efficient method of government finance would be provision of money out of general revenues. True, this would lead to cuts in programs currently paid for by those same federal general revenues (absent increases in taxes) but it would also spread the burden throughout society. Private businesses could still be counted on to pay some of the costs, but how they raised the revenues to do so would be of no concern to government. The most efficient way for government to enforce private spending is through general regulatory requirements, letting businesses figure out their own ways of fulfilling these requirements.

Implications and Conclusions

Even before the attacks of September 11, 2001, a number of ideas for improving seaport security had been proposed. These included developing port security plans, developing new ways to track cargo, pushing the borders of the United States out and sealing the supply chain, designating a lead agency for port security, and using public-private partnerships to carry out security tasks.[19] The various efforts generating these ideas culminated in U.S. Senate Bill 1214, introduced six weeks before the September 11 attacks by Senator Ernest F. Hollings of South Carolina and cosponsored by Senator Bob Graham of Florida.

---

[19]Before the September 11 attacks, supply chains for waterborne commerce were extremely porous. It was very easy to tamper with goods en route, to insert or remove products inappropriately from containers. Sealing the supply chain implies the plugging of these holes, securing the cargo and integrity of shipping containers from tampering.

In general, these port security efforts lacked urgency. In at least one case, there was a belief, without any supporting evidence, that implementation of port security measures would not need to be mandatory because ports would voluntarily adopt them as good business, with savings more than offsetting expenditure.[20]

After September 11, the government discovered the urgency. The Hollings bill formed the heart of the November 2002 Maritime Transportation Security Act, for which the Coast Guard serves as lead agency. U.S. Customs and Border Protection began the Container Security Initiative, intended to extend the borders of the United States out and seal the supply chain, and the Customs-Trade Partnership Against Terrorism, intended to seal the supply chain in partnership with the private sector. Other efforts to track and screen cargo were started, as was the grants program to help pay for selected port security measures.

The first wave of security programs created important barriers to terrorism, caused all participants in the maritime logistics community to think more carefully about security, and started the learning process for government agencies charged with securing the nation's ports. Two facts about security provision were apparent throughout these efforts, but these increased in prominence as people strove to implement security mandates.

First, it has been impossible to do everything at once. The effort to protect the nation quickly produced a kind of security policy congestion, with limited staff, money, and time resulting in slippage in schedules and implementation. For example, lack of time available to top management at the Department of Homeland Security is one cause for delays in implementation of an identification card for transportation workers.[21]

Second, there has been recognition throughout the process that strengthening one target necessarily means making other potential targets more vulnerable. Increasing the difficulty of slipping a bomb into a container increases the likelihood that someone might try to bring it into the United States in a yacht, or ship it to Mexico and bring it into the

---

[20]U.S. Department of Transportation (1997).

[21]U.S. Government Accountability Office (2004), p. 16.

country by truck. Or, with strong enough port security measures, terrorists might change their target focus from ports to the rail system or to shopping malls.

These two issues suggest that with the significant port security experience gained since 2001, it is appropriate to take stock of security efforts, formally analyze these efforts, and redirect programs and actions as needed. Well after September 11, policymakers are uncertain about the level of security we now have. Addressing Robert Jacksta, a Customs and Border Protection official, at a June 2005 hearing,[22] U.S. Representative Bob Filner of San Diego made clear his doubts about the C-TPAT program: "I think you should be saying, look, these are the challenges, help us meet those challenges, not tell us how everything is fine, because everything is not so fine."

Assessing the level of program implementation and security is difficult because it requires detailed knowledge of programs and of actions officials are actually taking. This report's study of emergency response at the ports of Los Angeles and Long Beach provides an example of such knowledge. It shows that there is progress but that the progress is slow and large gaps in program design and implementation remain.

The research in this study suggests a number of steps that the U.S. and state governments can take as they seek to strengthen the homeland security effort. The biggest threats to the United States from the maritime supply chain are from containers. Although an attack on a port could prove very costly, the infiltration of a nuclear weapon into some other location in the country using a container could prove even more costly. This suggests that the government should focus its efforts on sealing the supply chain and improving targeting abilities—while not neglecting lower-cost actions to make the ports and their perimeters more difficult targets.

Furthermore, a rapid response and economic reconstitution plan could minimize damage from either an attack on a port or an attack using the maritime supply chain. How the government reacts to the

---

[22]Robert Jacksta is Executive Director of Border Security and Facilitation, Office of Field Operations, U.S. Customs and Border Protection (Federal News Service, 2005b).

many problems created by an attack could be as important as how well it anticipates those problems, given that it cannot stave off terrorists with certainty. Strengthened recovery plans could return the economy to full activity quickly and prevent the population from panicking, breeding more trouble.

Second, given that no one measure can provide 100 percent security against the shipment of terrorist materiel in containers—or even terrorists themselves, since they have been found to travel by this means—the layered response being implemented is indeed the right way to proceed. The chief issues here are whether there are enough inspection points, or layers, and whether the current layers add enough security to justify their cost and the drag on commerce that they may cause.

Third, better policy guidance is needed. The U.S. government has demanded the implementation of multiple programs simultaneously, without setting priorities. This leaves the setting of priorities in the hands of senior government officials, who may have fine judgment but who also can be unfairly blamed by politicians for mistakes they may make in the absence of political guidance. Responsibility for program priorities belongs to elected officials—first to the federal executive branch and its agencies for designing strategy and implementation and to the Congress to allocate sufficient money to meet national goals. But even at the state and local levels, there is room for priority-setting, especially in the design of incident response and in ensuring a risk-based allocation of money and personnel.

Also as part of better policy guidance, a more coherent technology policy will help bring about increased security and economic benefits. Parts of this policy include the encouragement of technology development by the private sector, the purchase of commercial technology and subsequent modification for security purposes—rather than the special development of new security technology—and encouragement of greater international collaboration in technology development.

Fourth, response and recovery merit more attention. If there is an attack on the maritime system, a complete shutdown of that system could cause far more harm than the initial attack on one part of it. Plans

for reconstituting the system—and with it the economy—could also serve as a disincentive to terrorism attacks. Terrorists have been shown to direct their attacks at those targets where they are more likely to achieve their aims.[23]

Finally, the U.S. government should reconsider the level of staffing and funding devoted to port security efforts. Under current programs, 12,000 facility and vessel security plans and more than 5,600 C-TPAT plans will need monitoring (with the number of C-TPAT plans steadily rising). The U.S. Coast Guard has gained a large set of new duties that need staffing. New technologies need developing. Customs officials must review large amounts of new information to target high-risk containers. Personnel from the Coast Guard and other parts of the government need training in tasks previously unknown to them. Finally, new security equipment will need maintenance, repair, and upgrading. Efficiency can go only so far. As Senator Olympia Snowe of Maine said at a recent hearing:

> The Coast Guard should no longer have to say we can do more with less. We've heard that consistently before this committee, time and again. Frankly, I think it's a phrase that we ought to remove from the vocabulary. I well recall a past commandant saying that doing more with less will evolve into doing everything with nothing. Obviously we all refuse to accept that philosophy and that rationale.[24]

In port security, as in homeland security more generally, the issue is not only whether the government or the private sector will pay for increased staffing, inspections, and technologies. The issue is also whether—in the absence of renewed political will or an energizing event, such as an actual attack on the ports or a bomb found in a container—security will be implemented in a way that justifies all costs of the new security measures.

---

[23]Enders and Sandler (1993).

[24]Senator Olympia Snowe of Maine at a June 2005 hearing on the U.S. Coast Guard's capital equipment investment plan known as the Integrated Deepwater System (Federal News Service, 2005a).

References

Aegis Defense Services Ltd., *Aegis 2005 Terrorism Report*, London, December 10, 2004.

Agence France Presse, "Text of Laden's Latest Recording on al-Jazeera," December 28, 2001, available at indiainfo.com (as of November 2005).

Aljazeera.net, "Suspect Killed in Saudi Raid," April 5, 2005.

American Association of Port Authorities, "North American Port Container Traffic 2004," Electronic Database, Alexandria, Virginia, 2005.

Chertoff, Michael, "Statement by Secretary of Homeland Security Michael Chertoff before the House Appropriations Homeland Security Sub-Committee," Washington, D.C., March 2, 2005a.

Chertoff, Michael, "Remarks for Secretary Michael Chertoff, U.S. Department of Homeland Security, George Washington University Homeland Security Policy Institute," George Washington University, Washington, D.C., March 16, 2005b.

CNN.com, "Saudis: Al Qaeda 'Big Fish' Killed; 4 Killed or Caught on Most-Wanted List, Says Government," April 6, 2005.

Decker, Raymond J., "Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts," Testimony Before the U.S. Senate Committee on Governmental Affairs, GAO-02-208T, Washington, D.C., October 31, 2001.

Enders, Walter, and Todd Sandler, "The Effectiveness of Antiterrorism Policies: A Vector-Autoregression-Intervention Analysis," *American Political Science Review*, Vol. 87, No. 4, December 1993, pp. 829–844.

Federal News Service, Inc., "Hearing of the Fisheries and Coast Guard Subcommittee of the Senate Commerce, Science, and Transportation Committee; Subject: The Coast Guard's Revised Deepwater Implementation Plan," June 21, 2005a.

Federal News Service, Inc., "Hearing of the Coast Guard and Maritime Transportation Subcommittee of the House Transportation and Infrastructure Committee; Subject: Implementation of the Maritime Transportation Security Act," June 29, 2005b.

Flynn, Stephen E., *America the Vulnerable: How Our Government Is Failing to Protect Us from Terrorism*, HarperCollins Publishers, New York, New York, 2004.

Interagency Commission on Crime and Security in U.S. Seaports, *Report of the Interagency Commission on Crime and Security in U.S. Seaports*, Washington, D.C., Fall 2000.

Marine Transportation System Task Force, *An Assessment of the U.S. Marine Transportation System: A Report to Congress,* Washington, D.C., September 1999.

Office of Homeland Security, *FY2005 Homeland Security Grant Program: Port Authority Guidance*, Sacramento, California, July 27, 2005.

Office of Homeland Security, Governor's Office of Emergency Services, and California Service Corps, Office of the Governor, *FY05 Homeland Security Grant Program: California Supplement to Federal Program Guidelines and Application Kit*, Sacramento, California, January 26, 2005.

O'Hanlon, Michael E., Peter R. Orszag, Ivo H. Daalder, I. M. Destler, David L. Gunter, James M. Lindsay, Robert E. Litan, and James B. Steinberg, *Protecting the American Homeland: One Year On*, Brookings Institution Press, Washington, D.C., 2003.

Ransdell, Tim, *Federal Formula Grants and California: Homeland Security*, Public Policy Institute of California, San Francisco, California, 2004.

U.S. Army Corps of Engineers, *U.S. Foreign Waterborne Transportation Statistics Databank, Final 2003,* Alexandria, Virginia, June 2005.

U.S. Department of Homeland Security, "Remarks by Homeland Security Secretary Michael Chertoff at a Press Conference on the Fiscal Year 2006 Urban Areas Security Initiative Grants," Washington, D.C., January 3, 2006.

U.S. Department of Transportation, *Port Security: A National Planning Guide*, Washington, D.C., 1997.

U.S. Department of Transportation, *America's Freight Transportation Gateways: Connecting Our Nation to Places and Markets Abroad*, Bureau of Transportation Statistics, Washington, D.C., 2004.

U.S. Government Accountability Office, *Review of Studies of the Economic Impact of the September 11, 2001, Terrorist Attacks on the World Trade Center,* GAO-02-700R, Washington, D.C., May 2002.

U.S. Government Accountability Office, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program,* GAO-05-106, Washington, D.C., December 2004.

U.S. Government Accountability Office, *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security,* GAO-05-404, Washington, D.C., March 2005a.

U.S. Government Accountability Office, *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts,* GAO-05-557, Washington, D.C., April 2005b.

2. Ports, Trade, and Terrorism: Balancing the Catastrophic and the Chronic

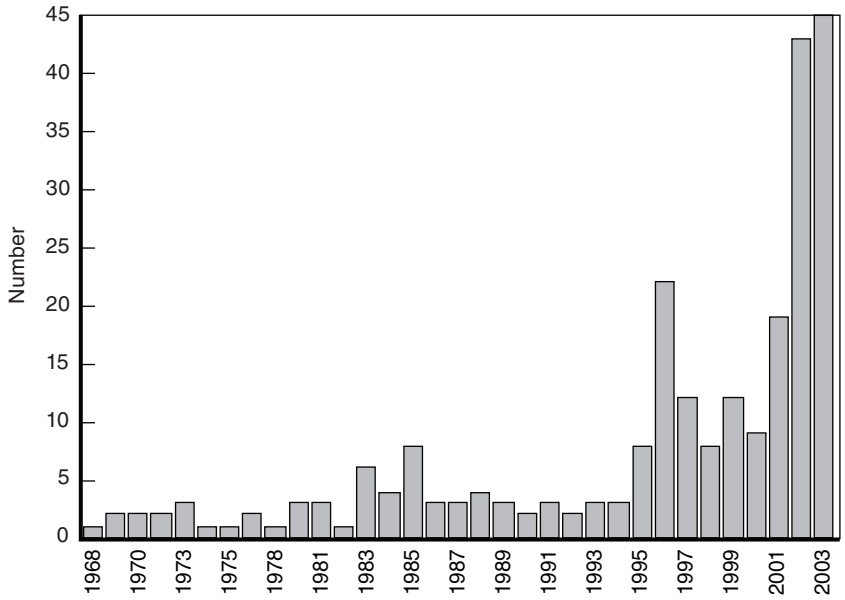
Edward E. Leamer and Christopher Thornberg
UCLA Anderson Forecast

Introduction

The number of attacks on U.S. interests, at home and abroad, rose substantially after 1995 (Figure 2.1), but the September 11, 2001, attacks on the World Trade Center and the Pentagon stand out as a pivotal moment when it became clear that the United States needed new national security measures, both to reduce the likelihood of new attacks and to reduce the damage of any future attacks.

Such security measures should result from careful choices. The best way to make these choices is one that compares the benefits of less-frequent, less-extreme terrorist events to the costs of security measures required to prevent them, including the direct costs of equipment and personnel and the indirect, non-pecuniary costs such as long waiting lines at airports. Efficient security measures are those whose marginal benefits equal or exceed marginal costs.

In this chapter, we perform the benefit part of this cost-benefit calculation for security measures at the ports of Los Angeles and Long Beach. An attack on the ports could in theory cause substantial economic damage, in addition to the loss of lives and property, by interrupting supply chains and idling workers in the manufacturing, wholesaling, and retailing sectors. In principle, these lost sales and lost earnings could be subject to a multiplier effect, as those directly affected spend less and thus reduce sales and earnings for those not directly affected. In the extreme, this might mean a national or regional



SOURCE: U.S. Department of State (2004).

Figure 2.1—Annual Number of Significant Terrorist Attacks on the United States, 1968–2003

recession. Additionally, nations whose economies depend on maritime exports to the United States, especially those in Asia, would feel the effects of reduced demand for their products.

This chapter estimates the effect of a disturbance to the flow of goods through U.S. ports by examining past events that have disrupted port operations in a similar way, specifically, maritime labor disputes. Although the only recent labor disruption was the relatively short 10-day West Coast closure of 2002, there have been tumultuous periods in labor relations on the waterfront in recent years. There were major labor actions in 1963, 1964, 1969, and 1971. These work stoppages—mainly along the East and Gulf Coasts but including at least one affecting West Coast ports—lasted between 30 and 70 days. During these, the total national value of monthly imports fell by as much as 40 percent. Exports were affected even more, with one-month declines of up to 66

percent—this during a period when the United States regularly exported more goods than it imported.

Of course, a labor action is not the same as a terrorist attack; labor actions can be anticipated to some extent, whereas lack of anticipation is intrinsic to terrorist attacks. However, similarities remain. The labor actions of the sixties and seventies were often marked by wildcat strikes and work slowdowns, deliberately created to reduce or prevent mitigating actions on the part of the companies involved. Furthermore, there cannot now be an unexpected, surprise terrorist strike at U.S. ports. Because of the terrorist threat, many businesses have put in place redundancies and contingencies that will help mitigate the disruption caused by a port attack, just as they undoubtedly did in anticipation of the port strikes that loomed in the 1960s.

Furthermore, it is our understanding from interviews with experts, that it is highly unlikely that the physical damage from an attack would be enough to close the combined ports of Los Angeles and Long Beach completely. The size of the port complex and the large amount of excess physical capacity would make it nearly impossible for a conventional attack to stop or even reduce substantially the amount of cargo that currently moves through the ports—as long as authorities intervened to allow displaced shippers to use other parts of the complex. The port might nonetheless be shut down if the dockworkers refused to work or were prevented from working by the government. Such a directive might affect all the ports on one or both coasts.

Although the United States is considerably more trade-dependent today than in earlier periods, this potential vulnerability is offset by a number of factors. One is the shift from ship to aircraft for delivery of many high-value, time-sensitive goods, particularly on the export side. Second, countermeasures to a terrorist strike, such as increased inspections of containers, may be more onerous for imports coming from uncertain ports than for exports packaged in the United States. And although a widespread labor action would stop most maritime trade completely, a terrorist strike would only slow trade rather than stop it.

When added together, these factors mean that the disruption to the flow of goods as a result of a current terrorist attack could be roughly similar in size to the effect of a major port strike in the 1960s.

Therefore, we feel that these historic labor actions correspond closely enough to the kind of port disruption that a terrorist attack might bring to tell us a lot about the probable effect on the national economy of a terrorist attack on the ports.

We will show how these labor actions are visible in the import data and export data of the period. In all cases, there was a small increase in import volume before these actions, a drop in volume during the action, and a large surge in import volume after the dispute was settled. Because of the size of that postdisruption volume surge, the overall loss of trade during a labor action was very small and in some cases nonexistent. Trade was postponed but not lost.

Nor are the adverse effects of labor actions evident in other data that we have examined, including data reporting production and employment. Our results show quite conclusively that the effect of these past strikes on the greater economy was negligible.

This is testimony partly to the great resilience of a modern economy. Short interruptions to supply chains can be mitigated fully by drawing down inventories, especially if they were built up in anticipation of the event. When inventories are depleted and delivery essential, cargo can be shifted to air or land through a neighboring economy. Somewhat longer interruptions can be compensated for through a temporary shift to domestic suppliers—an especially easy alternative if supply chains have built-in redundancies that allow the needed flexibility. Some consumers at the end of the supply chain may have to wait a while or pay higher prices. The sale—and profits—may be postponed, but they are not prevented.

Our results do not say that no business was hurt by port labor actions or that profits were not adversely affected by the increase in transaction costs. Some industries, some firms, and some regions were surely adversely affected. Nor do we claim that a terrorist attack on the ports and the resultant disruption to the supply chain would not harm any region or company—certainly some firms and regions would be affected. However, as is often the case in a modern complex economy, when one industry or area suffers as a result of some economic disturbance, another prospers as a result of an offsetting shift in demand: There are winners and losers. Our main point here is that these past

disruptions were insufficient to cause any noticeable change in the aggregate flow of the economy: Either the losses were small compared with the overall economy or they were largely offset by gains elsewhere. We believe that the same would be likely after a terrorist attack on a port: Its effects are not likely to show up other than in imports and exports.

Of course, our study presumes a short- to medium-term disruption to the supply chain, limited to approximately 60 days, as were the labor actions we study. It is our belief that lengthier disruptions are highly unlikely as long as the government is prepared to intervene. We conclude that the cost-benefit analysis of port security can safely discount the secondary economic costs that might be caused by a port disruption.

Benefits calculations should concentrate mostly on the lives and property that are directly at risk. Mitigating efforts would include plans to reduce the potential economic disturbance in the event of a port attack, including a risk-assessment program to separate safe from dangerous cargo, a way to prioritize imports in order of economic importance in the event of restricted capacity, and resources to create temporary port facilities or to rapidly expand other, existing facilities.

The first section details the cost-benefit analysis of port security. Next, we show that neither the attacks of September 11 nor various natural disasters caused economic slowdowns, contrary to a common, alarmist assumption that leads many to predict that terrorist attacks on ports would cause economic recessions. The section following that summarizes what we have learned about the possible effects of a port attack on the operations at the ports of Los Angeles and Long Beach and explains why an attack is unlikely to idle cargo throughput, provided the response is adequate. The next section then describes the effect of historical port strikes on the U.S. economy. The final section summarizes and presents conclusions.

The Cost-Benefit Analysis of Security

A security enhancement adds net value if the present value of the benefits in terms of reduced potential damage to the economy from terrorist attacks exceeds the present value of the up-front and ongoing costs. The ongoing costs of security are made up of the direct and indirect resources used to reduce the chance of a substantial terrorist

attack. The direct costs are the expenditures on the necessary equipment and manpower needed to provide the additional protection. Additionally, we have to factor in the increase in transaction costs that security measures often impose on third parties—typically those being protected. For example, the time cost of airport delays should be included in any discussion about increasing security at those airports. To some extent, a tradeoff between the direct and indirect costs of security is understood. This is why airports invest in expensive metal detection machinery rather than simply strip-searching every passenger. In the case of port security, the secondary costs would include increased transit times, security compliance, and greater delivery uncertainty.

The secondary losses that we study stem from disturbances to the normal supply chains and also from behavioral changes caused by changes in the psychology of consumers. For example, if consumers decided to stay glued to their television sets for several months after an attack and stopped rushing to the malls with their credit cards, that would disrupt the retail end of the supply chain as much as or more than the likely infrastructure damage. An example would be the sharp drop in air travel after the September 11 attacks, which seriously affected airline revenues. Another form of secondary losses comes from all the costs that individuals bear to prevent or to insure against future damage.

It is easy, however, to overestimate these secondary effects. We have to be careful about distinguishing between events that cause business to be delayed and those that cause business to be cancelled. Very short-run disruptions to trade—whether by severe weather, traffic problems at the port, or a small terrorist attack—have almost no net effect on the economy, since the disruptions caused are little more than what happens during the normal, random, day-to-day life of commerce. Small delays have no measurable effect, and firms very often have excess capacity in order to deal with unexpected fluctuations in demand. And although consumers might stop flying as a result of an incident, they may instead begin to buy more cars with the money they did not spend on air travel. Losses in one place may be offset by gains elsewhere. Only sustained shocks to the economy will have any permanent effect on the economy, and here we must be careful to recognize that the economy is composed of conscious agents who will adjust plans and use resources in different

ways to mitigate damages. We must not underestimate the resilience of a free-enterprise economy.

Most Shocks Do Not Cause Recessions

September 11 Did Not Cause the 2001 Recession

There is a strong tendency to blame too many secondary effects on disasters. A good example of this phenomenon is found in the September 11 attacks on New York and Washington, D.C. In the days after the attacks, the rhetoric regarding the potential effect on the national economy was both loud and wrong. The theory proposed by many analysts and journalists was that psychologically fragile consumers in the United States would suffer a crisis and stop spending, driving the economy into a deeper recession. Support for this theory came from the first Gulf War, which supposedly caused a similar consumer crisis of confidence that in turn drove us into a recession in 1990. For example, the *Wall Street Journal* reported on September 13, 2001:

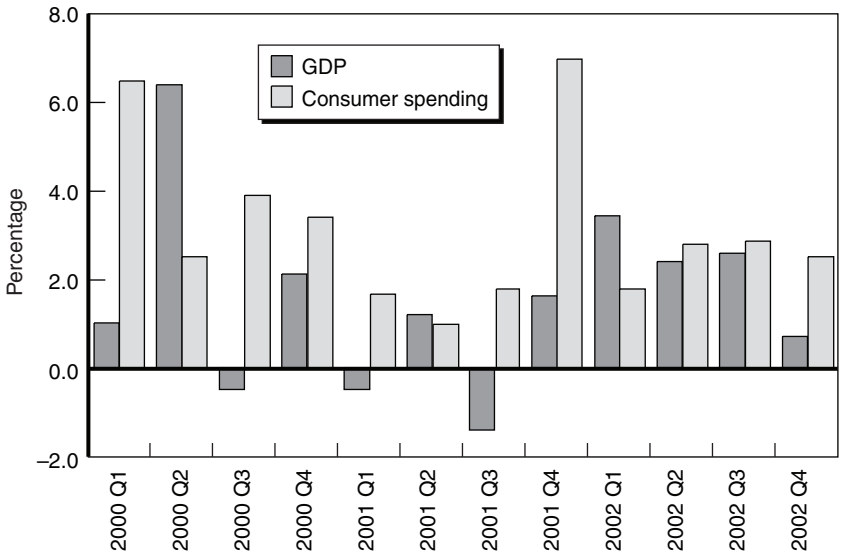
> "Past shocks to America's sense of security, such as the Oklahoma City bombing or the Gulf War, have prompted consumers to pull back temporarily on major purchases and other discretionary spending," said Richard Curtin, director of surveys of consumers at the University of Michigan. He expects a similar reaction now, which could mean a rough time in the next several weeks for the economy, which was already struggling with rising jobless rates and high consumer debt burdens. "We were teetering on the edge, and this might well push us over," said Mr. Curtin.

This hypothesis ignores the facts and completely overstates the psychological fragility of American consumers. The 1990 recession was not caused by the first Gulf War at all. Residential investment and expenditures on consumer durables typically are leading indicators of the economy. When spending on these items begins to fall as a percentage of gross domestic product (GDP), this is a strong indication of an underlying weakness in the economy that will create a recession. Expenditures in these two sectors had dropped from 14 percent of GDP to below 12 percent of GDP in the three years preceding the 1990 downturn—and before the Gulf war. There has never been such a drop that did not eventually lead to a recession, with one exception—in 1967, when the economy was wobbling, appearing to be on the verge of

recession, the sharp increase in spending for the Vietnam War propelled the economy forward. This was just the reverse of what Mr. Curtin suggested.

Similarly, the U.S. economy did not slow down after the September 11 attacks; indeed, the economy was in the midst of accelerating its way out of the 2001 business-led downturn that had begun in the middle of 2000. And although consumer confidence fell sharply after the attacks, consumer spending in the fourth quarter grew at an unprecedented 7 percent seasonally adjusted annual rate (SAAR), one of the sharpest increases seen in the past decade (Figure 2.2). Unemployment did rise sharply after the event, but this seemed to be primarily an acceleration of the employment loss that would have been expected given the weak economic climate. This was especially true because labor markets were still overheated from the tech-fueled economic boom of the late nineties.

Retail sales did drop sharply in September 2001 but also rebounded sharply in October and returned to trend in November—business



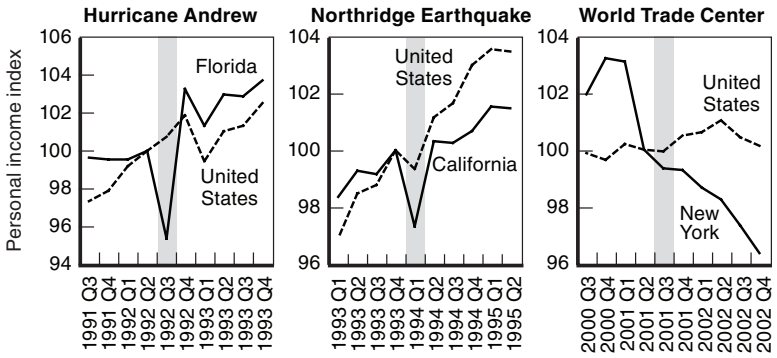
SOURCES: U.S. Department of Commerce (2006a, 2006b).
NOTE: Data are presented as seasonally adjusted annual rates.

Figure 2.2—Growth in Real GDP and Consumer Spending, 2000–2002

delayed, not business cancelled. Indeed, it is hard to find any evidence of an effect of the September 11 attacks on the aggregate economy, with the exception of that on the air travel industry. Even in that case, the industry was in deep trouble beforehand, with profit margins dipping into the red in the beginning of 2000—long before the attacks. Even then, it must be remembered that total consumer spending went up, so the dollars that were not spent on air travel went to some other part of the economy.

Natural Disasters Also Do Not Cause Recessions

More local effects of disasters are easier to see in the data. The three state charts in Figure 2.3 show indexes of the quarterly path of real personal income (adjusted for changes in the consumer price index) for substantial catastrophes in Florida, California, and New York. Hurricane Andrew, the Northridge earthquake, and the September 11 attacks each caused approximately $25 billion to $30 billion worth of destruction in each state's economy, in constant (2004) dollars. The charts give a rough approximation of the disturbance to the local flow of the economy—business disturbances should result in loss of economic output, and thus income. (Government transfers have been removed to exclude federal disaster relief payments.) In all three cases we also show personal income for the balance of the United States as a frame of



SOURCE: U.S. Department of Commerce (2005b).
NOTES: Government transfers not included. Index equals 100 quarter before event.

Figure 2.3—Indexes of Personal Income Around Significant Local Events

comparison. The quarter in which the disaster event occurred is highlighted.

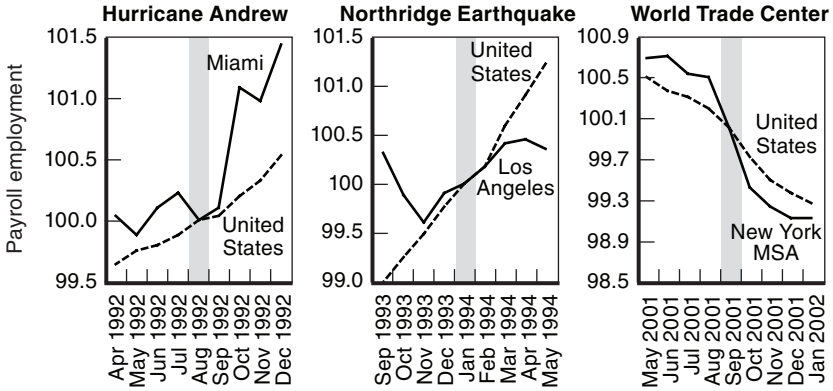
For Florida and California, the substantial decline in income flows during each disaster is clear, as is the rebound occurring after the fact. We can use U.S. growth (adjusted for trend differences) for the two quarters during and immediately after the event as the determinant of what would have happened to income if the event had not occurred. With this calculation a simple estimate of the net cost of the disaster on personal income can be created. For Florida, the loss in constant (2004) dollars is about $3.5 billion (about 1% of annual state personal income), whereas for California, the figure is about $4 billion (about 0.5% of annual personal income).[1] Secondary damage here seems to fall somewhere between 10 and 15 percent of primary damage. It is worth noting, though, that both states saw a $10 billion increase in transfer payments into the region, in the form of federal disaster assistance and insurance payments.

Interestingly for New York, there is not even a dip. Instead, the changes are dominated by the dramatic decline seen between the first and second quarter of the year, which of course was due to the collapse of the stock market bubble. The reason for this is likely, in the case of New York City, because the damage sustained was concentrated on a small area, whereas for Los Angeles and Dade Counties, the damage was more widespread geographically. Thus, the level of disturbance to the greater area was smaller. If anything, the slide resulting from the 2001 economic downturn seems to have slowed somewhat after September 11; this may be attributable to the $18 billion in new transfers that flowed into the city after the tragedy.

Income presents only one side of the picture. Employment presents another. Figure 2.4 shows indexes of non-farm payroll employment

---

[1]See Thornberg (2002) for details on these calculations and those regarding employment.



SOURCE: U.S. Department of Labor (n.d.a).
NOTE: Index equals 100 in month of event.

Figure 2.4—Indexes of Payroll Employment Around Disasters

(measured as of the 12th of the month) for Miami, Los Angeles, and the New York consolidated metropolitan statistical area (CMSA) around the three events, with the month of the incident set at a value of 100. Each event occurred in the midst of business downturns for the region and nation overall, so the equivalent data for the United States are included. For Miami and Los Angeles, where the income effects were visible, there appear to be mild or no employment effects at all. For Miami, there was mild growth in employment in September, and October saw a very large jump—almost 1 percent. For Los Angeles, in the midst of a weak economy caused by the collapse of the aerospace industry, employment continued along its slow growth path.

For New York, the CMSA employment numbers that include Long Island and New Jersey are used rather than the primary metropolitan statistical area (PMSA) numbers for the five-borough region to avoid calculating the movement of jobs out of Manhattan across the river. Employment in the CMSA began to drop off before September and continued to fall through January. Of course, the nation was also experiencing a loss of jobs as part of a downturn that began in 2000, but this was not reflected in the labor markets until March 2001. Even in this case, although it appears that there might be some employment effect from the September 11 attacks, it must be kept in mind that New

York, like the Bay Area and other centers of technology and finance, was going to suffer at a greater-than-average level, because these industries led the boom of the late nineties. A cross-section analysis of cities based on industry mix shows the New York PMSA actually losing *less* than the expected number of jobs given the initial industry mix of the economic region.

All this indicates that disasters, although tragic, are not recession-causing events. Recessions are caused by a sharp, substantial, and sustained reduction in spending by one or more segments of the economy. Typically, this segment is consumer spending on homes and durables, but not always. In the case of the 1953 recession, and in the case of the 2001 recession, Department of Defense spending on the Korean War, and business spending on equipment and software, were the respective segments that experienced reductions. Natural disasters might cause a sharp and substantial decline in consumer spending, but that decline is very short-lived. Within a month or two, there is more consumer spending, not less, because of repair and rebuilding activities. The hype of the effect of a disaster is typically much greater than the reality. Business is only delayed, not cancelled, and the economy can quickly get back on track.[2]

How Much Disruption to Supply Chains?

The appeal of an attack on the ports of Los Angeles and Long Beach from the point of view of a terrorist would be the potential secondary effects, not the direct loss of life or the destruction of physical assets. Although these ports are busy and have quite a number of employees and stock in the facility at any point in time, if the goal is direct destruction of lives and capital, there are more attractive targets with high population and asset densities such as Manhattan or perhaps Los Angeles International Airport. The ports, of course, have a fairly low population

---

[2]Of course, a sustained series of many terrorism attacks may have a recession-causing effect on an economy. The classic case occurred in Bosnia during the protracted civil war and the siege of Sarajevo in the 1990s. The tipping point of this recession is unclear. Israel has suffered from intermittent terrorism attacks for years, and there is little evidence that these have had much of an effect on the expansion of its economy.

density relative to many other locations. The primary damage of any attack would be proportionally small.

The secondary effects, conversely, might be substantial. There is little doubt that the Los Angeles–Long Beach port complex represents a critical node in the international supply chain (Table 2.1). More than 14 percent of goods by value imported into the U.S. economy flow through the two ports. They process more than 30 percent of all national maritime traffic alone. They also process a substantial share of exports—carrying 4.7 percent of total exports and almost 17 percent of maritime exports. The two ports process a variety of products, both final goods intended directly for consumption and many intermediate inputs needed by the nation's producers. Closing the ports would interrupt this traffic and presumably cause large disruptions in the supply chains for many firms. Such a closure could in turn lead to factory closings, layoffs, and in the end spark a substantial slowdown in the national economy.

A cursory look would seem to portend a dramatic, dangerous scenario, but a closer look at the facts suggests otherwise. From an input-output perspective, a wide variety of holes would be quickly created in the flow of production that would seem to lead to a very sharp downturn in economic activity. But our economy is not a mechanical system; it is an organic self-healing system, much like that of a human being: Large injuries take time to heal, but for the most part they do eventually heal. To continue the analogy, a port attack is only a cut on

Table 2.1

Value of Trade Through Los Angeles County Ports, 2003

	Imports ($ millions)	Exports ($ millions)
Total U.S. goods trade	1,282,000.0	726,400.0
Total U.S. waterborne	604,631.2	202,480.7
Port of Los Angeles	105,185.9	16,864.6
Port of Long Beach	$78,700.0	17,163.0
Ports as % of U.S. total	14.3	4.7
Ports as % of U.S. waterborne	30.4	16.8

SOURCES: U.S. Department of Commerce (2005a); U.S. Department of Transportation (n.d.).

the arm—quickly healed with little noticeable effect on the day-to-day functioning of the person.

Although the ports of Los Angeles and Long Beach certainly represent a primary infrastructure target in the United States, a complete shutdown of the ports is highly unlikely as a direct result of some physical attack. There are two reasons for this: the sheer physical scale of the facilities and the large amount of excess physical capacity (as opposed to human capital capacity) currently in place. As shown in the port map on p. xxiii, the two facilities take up approximately 12 square miles of space in a six-by-four-mile area. The complex is broken into a number of separate yards, each completely controlled by a number of independent, competing major shipping lines, each of which have substantial investment in the physical cranes and equipment on their property. Some of these yards are on Terminal Island, connected to the mainland by three road bridges and a railroad; others are on the mainland itself. There are multiple access points into the area as the map shows, including two highways. Even if these roads were shut down, it would be relatively simple to construct a temporary bridge to the island, and although it might have some implications for the movement of ships, no yard would be effectively isolated.[3]

Conventional weapons would be able to damage, at best, only a small portion of the complex, and would be unable to isolate a substantial portion of the port given the multiple access routes into and out of the area. Even a so-called "dirty bomb" could cover only one or two square miles of area with radioactivity. Given the location on the water, winds would quickly blow most of the radioactive materials away, leaving even most of the initially affected area quickly reusable. The only known weapon that could take out an area of this size for an extended period of time would be a nuclear weapon. It seems more likely that the

---

[3]Temporary bridges are used in many circumstances surrounding disasters, construction, and military action. For example, the Bailey Bridge Company (www.baileybridge.com/) produces bridges that can be set up in days for use in construction zones. This company began by providing pontoon bridges in World War II that could carry tanks that commonly weigh 30 to 35 tons. The U.S. Army has a special group, the 299th Engineer Company (Multi-Role Bridge Company), which specializes in building pontoon bridges. The 299th built one over the Euphrates River in 2003 during the Iraq conflict. This float bridge was 185 meters long.

target of such a horrific device would be a densely populated area, not a port.

Given that it is unlikely for the entire port complex to be closed for an extended period as a result of an attack, the next question is what would happen if an attack instead destroyed only a portion of the port facilities. Under this scenario, the effect on trade and any secondary effects would depend on the ability of the functioning portions of the port to pick up the slack. Although the stories of congestion at the port and ongoing plans for expansion seem to imply that the ports are running close to or at capacity, they are not actually near capacity—at least not from a physical perspective. Most of the year, the various facilities run only one shift per day. During periods of increased trade activity, they may run two or, in the most desperate of circumstances, three. Multiple shifts, however, are very unusual because of the increased labor costs and work restrictions of labor agreements. But if the manpower were available, each yard in the facility could likely move at least twice as much merchandise through if it ran 24 hours a day.

Indeed, this point has been made clearer than ever in recent months as local officials have moved decisively to reduce midday congestion around the ports by charging a fee to companies that want to move goods and products into and out of the ports during normal business hours. It is understood that the port infrastructure is largely underused during most of the day, and that economic incentives are needed to use it more efficiently.

If a portion of the complex were closed as a result of damage to its transportation infrastructure, it would be relatively simple to transfer the shipping into other facilities. We assume that in the event of a national emergency, competing shipping companies would share facilities.

The Problem Is With Labor

The true limiting factor at the ports is not physical capacity but human capacity—labor to run the cranes and to move goods and containers in and out of the yards. If a portion of the facilities were closed, labor shortages in other yards handling the extra traffic could be made up of crews brought in from the closed facilities or even from other port facilities on the West Coast, from emergency aid from the Coast

Guard or other military organizations, and eventually by new crews trained over the course of the succeeding weeks.

At the same time, a certain amount of shipping could easily be funneled through other West Coast ports with excess physical capacity. In the longer term, shipping could be rerouted to East Coast ports and to refitted West Coast facilities not currently able to handle modern containerized shipping. In short, although the cost of importing products would surely rise as a result of the logistical difficulties created, there is no reason to believe that trade would be substantially interrupted. For those industries that rely on imports to run their business, there would be extra costs in the short run. The longer the disruption the less these costs will be, as better solutions are found.

In our view, the true threat to the ports is not the physical damage to facilities, given the excess capacity in the system that could be used in the event of a true emergency. Rather, the true limitation is the unwillingness of labor to work under potentially hazardous conditions. The most dangerous scenario might occur as follows: A single conventional bomb goes off in a containerized shipment, killing or injuring a number of port personnel. The attack is followed by a threat that a number of other similarly rigged containers are on their way into U.S. ports or perhaps have already been offloaded and are awaiting transfer.

One result might be that work crews understandably would refuse to work until the government could assure some degree of safety. In another scenario, the ports could be closed not by labor but by the government. If the attack on the World Trade Center was an indication of what might happen in the wake of a serious attack, then the government itself might shut down U.S. ports while deciding how to handle the new crisis. This would imply that the government would have to put some sort of screening process into place rapidly by which safe containers could be separated from potentially dangerous ones, with a second physical screening to detect potential explosives in this latter category.

The result of this strategy would be a dramatic slowing of goods moving through the port—one that would not necessarily be limited to just one port but potentially to all ports of entry along the coast, since

terrorists are unlikely to be specific about their targets. In this case, the issue of mitigation becomes far more complicated for importers and for the government in general. How long would it take the government to be able to distinguish low-risk containers from those that are truly a threat? How could screening be done? How would traffic through the ports be prioritized? For firms that rely on products that flow through ports to keep their operations running, a number of important questions also arise. Could alternative suppliers within North America be found? Are there alternative routes such as by land through ports in Mexico or Canada or perhaps by air? As discussed below, these are important questions that should be answered now, not after an attack actually occurs.

Previous Port Closures Hold Lessons for the Present

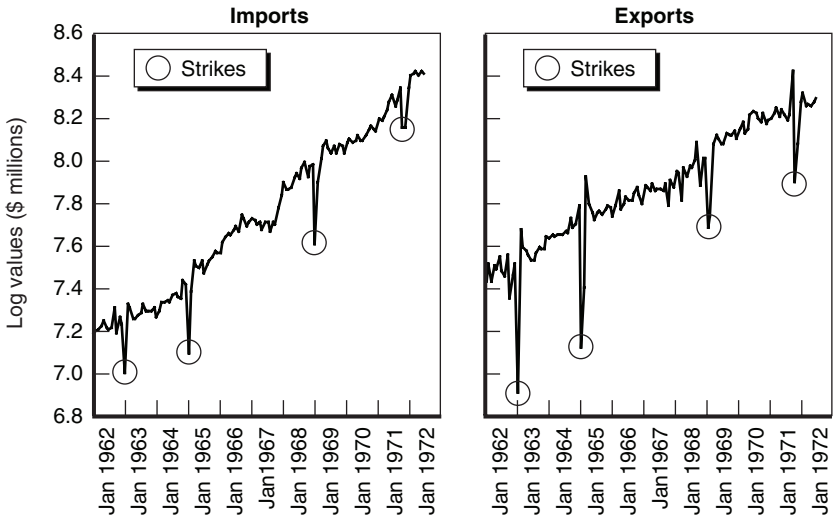
When economists trying to make predictions are faced with a long list of unknowns, they can either develop complex models to help answer the questions before them or look to historical events that might provide lessons for the future. The complex questions stemming from a terrorist attack on the port complex cannot be answered easily within a typical static input-output (IO) model, because the economy is flexible and will work to mitigate the potential damage caused by a supply chain disruption. Input-output models assume a mechanical structure in which a resource unused in one place remains unused. For example, there is an assumption that a laid-off worker will not try to find new employment, or that a factory, denied a critical component, will simply shut down instead of finding an alternative supplier. Of course, these assumptions are not true. Input-output models tend to highly exaggerate the true cost (and also the true benefits under other circumstances) of economic events.

When IO models cannot do the job, economists look toward similar episodes in the past to provide information about the potential consequences of some change in the economy. We believe that historical episodes more appropriately capture the patterns of adjustment that a flexible economy with adaptive businesses and workers will make in response to disruptions. We do not have any examples of a terrorist strike on U.S. ports, but there are some historical incidents of work

stoppages at ports that interrupted maritime trade in a fashion that seems similar to the disruption that a terrorist attack could potentially cause.

The last major labor-related port closure occurred in 2002, when West Coast ports were shut for 10 days. This event was unusual for recent times, but earlier in the country's history there were substantial maritime work stoppages—particularly in the sixties as ports began to introduce labor-saving technologies, especially containerization. There was a 35-day strike in late 1962 and early 1963, a 33-day closure in early 1965, and a 40-day strike in 1969. The largest work stoppage occurred in 1971, when the ports were closed on and off for more than four months, although the data show the actual effect on trade to be less than 90 days. Figure 2.5 shows how these events had a noticeable effect on trade flows into and out of the country.

It is distinctly possible that a port strike would cause less damage to the economy than a terrorist attack would. Unlike a terrorist attack, a port strike is predictable because lengthy labor negotiations occur ahead of time. Of course, a terrorist *threat* is predictable as well, even if the



SOURCES: U.S. Department of Commerce (various dates a).
NOTE: Data are seasonally adjusted.

Figure 2.5—U.S. Goods Trade and the 1960s Strikes

actual attack is not. The probability levels of an actual attack, by comparison, might be substantially smaller, thus leading to less mitigating reaction by business. However, the government typically does not intervene in the event of a labor action, whereas it would in the event of a terrorist strike. As a result, a strike or other work stoppage might cause a greater slowdown in traffic than a terrorist attack might.

One objection to this line of inquiry is that we are looking at labor disputes that occurred in the 1960s and 1970s, when the United States was less trade-dependent and in particular less dependent on the imports of parts and intermediate goods. In fact, goods trade is about 17 percent of GDP today compared to about 7 percent in the late sixties. Nonetheless, other factors indicate that although the percentage of overall trade was smaller in the sixties, U.S. ports represented a much more critical component of the supply chain. In that era, the ports handled a larger proportion of overall trade flows than they do today (Table 2.2). Nearly 70 percent of goods imports and 60 percent of goods exports moved through U. S. ports in the sixties, as measured by value. Today, the corresponding values are 50 percent and 25 percent. Besides the obvious importance of this in terms of a disturbance at the port, it also shows that the number of potential substitute routes for goods coming into the United States is larger than ever. Air transport, in particular, plays an increasingly important role, especially for high-value products. Ocean shipping today represents for the most part relatively low-value products (relative to weight) and those for which the supply chain is more

Table 2.2

Imports by Transport Type
(% shares calculated by value)

	Ship	Air	Land
1965	69.9	6.2	23.9
1975	65.5	9.2	25.3
1985	60.4	14.9	24.8
1995	51.2	21.6	27.3
2004	49.3	22.4	28.3

SOURCE: U.S. Department of Commerce (various dates b).

flexible given the vagaries of sea transport relative to air. And of course although international trade has grown with all countries, the largest trading U.S. partners were and remain Mexico and Canada. These two neighboring nations, with whom trade is conducted mainly by truck and rail, accounted for slightly less than a third of all goods trade in the 1960s, and today they represent something more than a third.

Furthermore, the labor stoppages of earlier eras had a dual effect on the economy because they stopped both exports and imports. For the terrorist scenario we lay out, we feel that such an attack would affect imports far more than exports, reducing the overall size of the shock to the economy. The shift in the composition of trade would also attenuate the effect on the economy. Non-petroleum industrial supplies made up 36 percent of all goods imports in 1967, whereas consumer and other products made up only 22 percent. By comparison, industrial supplies make up only 15 percent of imports now, whereas consumer and other goods make up 31 percent. If a critical component of a manufacturing line fails to arrive, that might cause widespread disruption, but the lack of yet another lamp made in China on Wal-Mart shelves would not. Indeed, such disturbance to the patterns of trade flows could create additional consumption demand for products made here—temporarily improving the job markets in manufacturing. Additionally, domestic production of goods is now a smaller proportion of GDP, implying that a disturbance to supply chains into the goods sectors would have a smaller overall effect on the economy. In the sixties, the production of goods made up nearly half of the economy. Today, it is far less than a third, as services have been the primary growth portion of the economy.

Finally, communication and information-sharing is far easier than it was 30 years ago, making it easier for firms to find alternative suppliers or alternative routes for products in the event of some disturbance to their supply chain. The result is that firms are more nimble and more capable of efficiently handling problems with their supply chains, not less. Other efficiencies include shorter production runs and an increase in firms in the supplier business that now tout their ability to provide special needs in short order. As for our just-in-time economy, although it is true that the inventory-to-sales ratio has fallen from 1.69 to 1.36 for

manufacturing industries in the past 40 years, it has actually increased for the wholesale and retail trade sectors (Table 2.3).

All these factors indicate that although past port shutdowns may not be the perfect example of the effect of a terrorist attack on our ports today, they should be very informative. We might consider this a low estimate for the potential for disturbance to the aggregate economy, but it is certainly a solid estimate.

Table 2.3

Inventory-to-Sales Ratios

	1960–1965	1995–2000
Manufacturing	1.69	1.36
Wholesale	0.88	1.30
Retail	1.04	1.41

SOURCE: U.S. Department of Commerce (2001, 2006c, 2006d).

Previous Port Shutdowns Have Not Had a Great Effect on the Economy

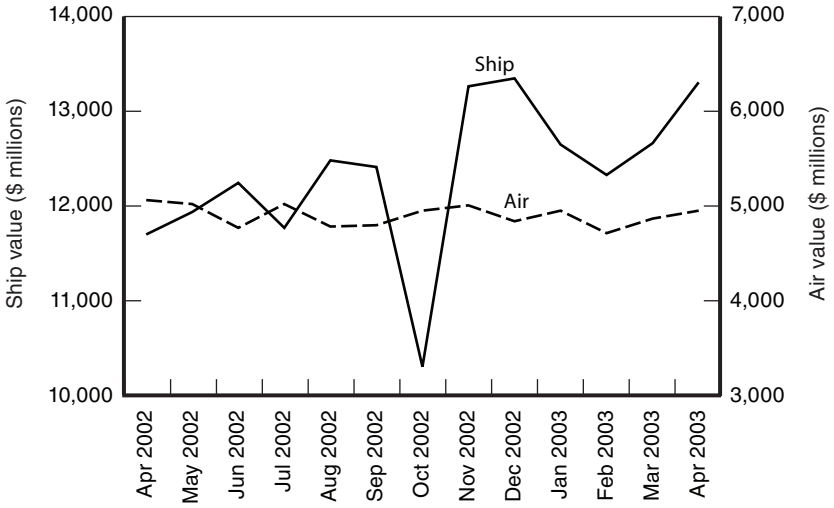
On September 29, 2002, the dockworkers on the U.S. West Coast were locked out of the port facilities after a protracted period of failed contract negotiations. The ports remained out of operation for 10 days. A widely quoted figure was that the closure would cause a loss of $1 billion per day in damage to the economy. Although it was in error, this figure still circulates on the Internet as a "good" estimate of the cost of delays in trade. Another estimate was a $19 billion loss for the 10-day period.[4] Most of these assessments ignored the mitigating responses that a modern economy is capable of producing and missed the fact that the length of the closure would play a large role in determining the extent of the damage to the broad economy. To express this another way: There is a difference between business lost and business delayed.

There is little doubt that the 10-day closure had a noticeable effect on trade flows. The following graphs show the seasonally adjusted

[4]Gaudette (2002). The firm that made the initial $19 billion estimate later said that the shutdown cost the economy $15.6 billion (Martin Associates, 2005).

patterns of imports through California customs districts around the time of the closure. The level of trade fell by nearly 20 percent from September to October, followed by a large rebound in November and December (Figure 2.6). Export trade value from California by ship is smaller than import value by a factor of more than three. In absolute terms, exports fell by the same amount as imports in October, about $2 billion. In relative terms, the percentage was much larger, and November did not see a large rebound. It seems as if exports may have been more affected than imports by the closure.

Shifting time-sensitive, high-value cargo to air is one possible way to mitigate a port interruption. But in 2002, the state's airports did not seem to pick up any of the lost traffic. It seems likely that most of the time-sensitive high-value cargo was already being shipped by air, and given the expected brevity of the lockout, not much cargo needed to be shifted to air transportation. (It could also be the case that air cargo is capacity constrained in the short run or that imports by air flew directly to their intended destinations, outside the state.)

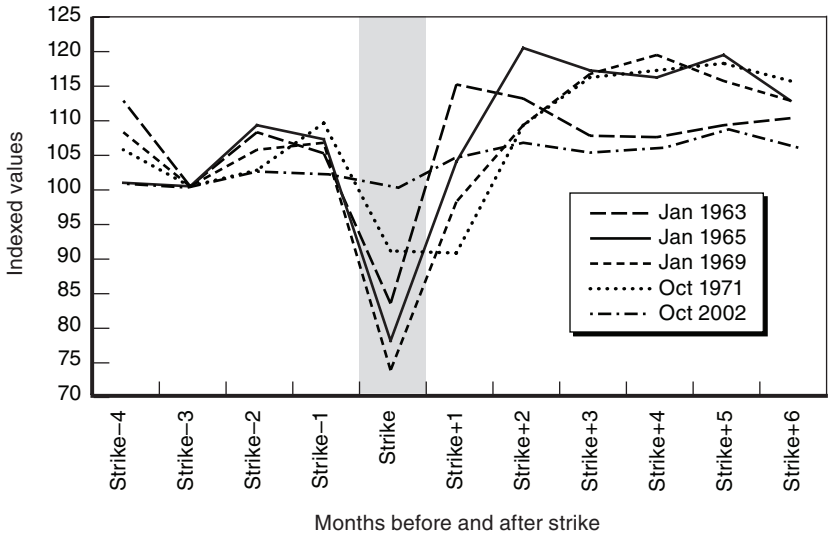


SOURCES: U.S. Department of Commerce (various dates a).
NOTE: All values are seasonally adjusted.

Figure 2.6—Imports Through California Customs Districts, 2002–2003

Although the effect of the 2002 lockout can be seen in local import and export data, at the national level, the proportional decline in imports was much smaller than it was in previous labor actions (Figure 2.7). These occurred across the United States, affecting the flow of goods across the nation, but their effects were particularly notable in the East Coast and Gulf states. Ports in these regions carried about two-thirds of national cargo in terms of monetary value and 80 percent in terms of gross weight. In 1965 and 1969, total imports (including imports carried by all modes of transport) declined almost 25 percent at the national level during the month of each labor action. In 1971, trade declined about 10 percent for each of the two succeeding months of the labor action, and then recovered. In contrast, the 2002 lockout saw at most a decrease of only a few percentage points in total imports at the national level.

Of course, over the last four decades there has been an overall increase in the U.S. economy's dependence on trade. In 2002, the United States was importing an amount of goods equivalent in value



SOURCES: U.S. Department of Commerce (various dates a).
NOTE: Index equals 100 in the Strike-3 period.

Figure 2.7—National Imports of Goods During Previous Port Shutdowns

to roughly 11 percent of GDP; in the 1960s, goods imports were only 4 to 5 percent of GDP. Thus, the larger percentage changes in trade in these earlier periods are offset by the import fraction of GDP. Still, these earlier events saw a reduction in trade in goods of an amount close to 1 percent of GDP. The October 2002 event saw a temporary reduction in imports by about one-third, also amounting to about 1 percent of GDP.

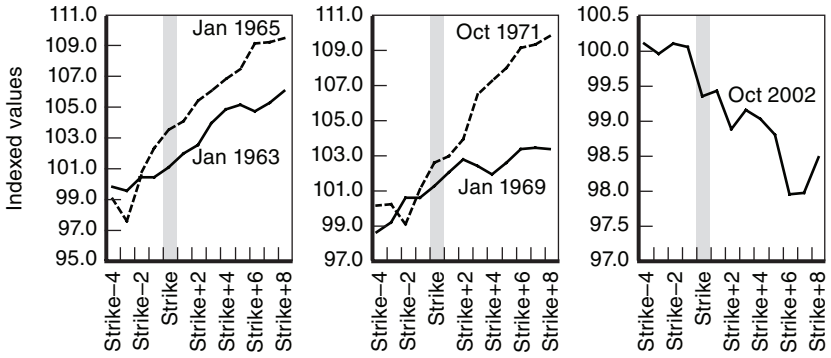
The economic shocks of the earlier labor disruptions were much larger overall than that of 2002 but the rhetoric was similar to that of the 2002 event. Consider some of the following headlines and reports from the *Wall Street Journal*:

- "Dock Strike Losses in Revenues and Wages Put at $400 Million" (January 8, 1963).
- "The Federal Maritime Administration estimates the strike is costing the U.S. economy $67 million a day; on this basis the loss is already at $2 billion" (February 9, 1965).
- "Impact of 21-Day Dock Strike Is Spreading; Costs Incurred Seen Leading to Price Rises" (January 9, 1969).

Adjusted for inflation, these are big numbers—that $2 billion in direct costs tallies in at $12 billion in today's values, on par with the claims being made about the 2002 lockout. So does the rhetoric live up to the hype? How did the trade disturbance affect the economy—specifically jobs and production?

We can start by taking a closer look at manufacturing production at the time of the five labor disruptions. Figure 2.8 shows indexed values of manufacturing output around the five labor actions. They show very little evidence that the port shutdowns had any significant effect on overall manufacturing output. For the 1963, 1965, and 1971 shutdowns, production continued along its trend, with any variations well within normal limits.

In 1969, a slowdown in production occurred three months after the strike ended. However, this was in the period leading up to the 1969–1970 recession, caused by other factors. The 2002 lockout does coincide with a general decline in manufacturing output, but this was a symptom of an economic slowdown that probably was not much affected by the



SOURCE: Federal Reserve Bank of St. Louis (1999).
NOTES: Index equals 100 in quarter before strike. Values are seasonally adjusted.

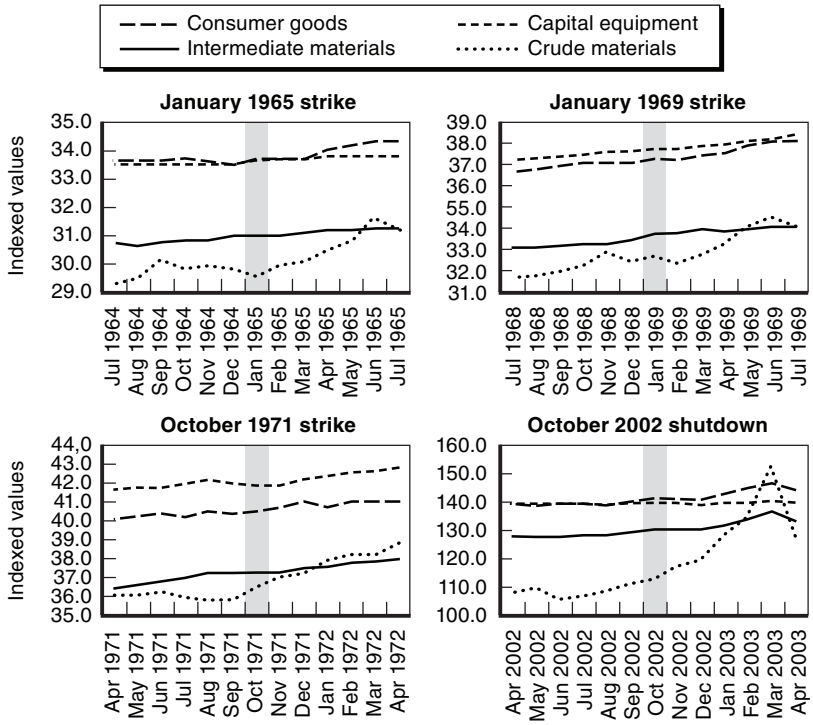
Figure 2.8—Value of Manufacturing Production During Port Shutdowns

lockout. Indeed the declines that started during the lockout continued until seven months after it had ended.

An alternative perspective might be available from the price data (Figure 2.9); disruptions at a port that cause serious disturbance to the economy should raise the price of intermediate and final goods. Producer price indexes (PPIs) for consumer goods, capital equipment, intermediate materials, and crude materials are shown around the 1965, 1969, 1971, and 2002 labor disputes in Figure 2.9. If these drove up prices at all, that fact cannot be seen in the data.

We find a similar lack of evidence of disturbance to the economy when we look at employment (Table 2.4). Specifically, we look at four sectors that would seem to be most at risk in the event of a disturbance at the ports—durable and non-durable manufacturing activity, wholesale trade, and logistics. Table 2.4 shows the patterns of average monthly changes in employment around these labor actions, for the six-month period before, the three-month period during, and the six-month period after.

Even a brief glance at the data shows that job loss is not associated with port labor actions. The only negative numbers in the table are those that occur in the context of a longer run trend in job losses. The



SOURCE: U.S. Department of Labor (n.d.b).
NOTES: Index equals 100 in 1982. Values are seasonally adjusted.

Figure 2.9—Producer Prices Around Past Labor-Related Shutdowns

most that can be stated is that the longest of the strikes may have caused a temporary slowdown in the pace of new job formation. However, these slowdowns were quickly reversed after the resolution of the dispute and were very small relative to overall trends.

Event Studies

"Eyeball estimation" is a good way to begin event studies of the effect of labor stoppages, but we need to do some statistical analysis to make sure that our eyes are not playing tricks on us. We report a simple empirical model of import flows and overall economic performance with indicator variables pointing to strike events. (The details of this analysis are included in the appendix at the end of this chapter.) The idea is to

Table 2.4

Employment Growth and Port Strikes

	January 1963	January 1965	January 1969	October 1971	October 2002
Durable goods					
Before	4.5	41.3	21.3	–2.8	–36.8
During	11.0	43.3	40.7	15.0	–50.7
After	30.3	124.3	15.7	114.3	–48.7
Non-durable goods					
Before	–4.2	14.8	9.0	2.8	–15.3
During	3.7	15.7	8.7	1.0	–21.7
After	6.3	25.3	5.0	32.0	–20.8
Transportation					
Before	–0.9	6.7	9.3	–4.1	–15.0
During	–0.9	7.5	4.3	–0.4	–1.0
After	5.1	12.7	20.0	–6.5	–13.9
Wholesale trade					
Before	0.2	9.3	8.9	5.4	0.3
During	7.2	10.1	7.1	9.9	1.1
After	5.9	20.0	19.6	27.7	–7.6

SOURCE: U.S. Department of Labor (2003).

NOTES: Before = six months before port closure; during = three months during; after = six months after. Monthly average, seasonally adjusted, in thousands.

empirically estimate the effect of the port shutdowns on the economy by first running a model in which the port shutdowns are included as a series of unexpected shocks to the economy and then taking out their effects in the context of an economic forecast to see if they had any significant effect on the economy. What is interesting is that there is no significant statistical evidence that the strikes had any effect on anything other than imports. And with imports, although the strikes certainly had an effect on the timing of shipments, they seemed to have had almost no effect on the overall level.

The differences between the forecast level of imports and the actual levels before, during, and after the shutdowns are shown in Table 2.5. Note that the number of months that the recovery period covers is being determined statistically, using the regression analyses laid out in the appendix. Months included were those that were statistically different

Table 2.5

Port Shutdown Effect on Trade

	January 1962	M	January 1965	M	January 1969	M	October 1971	M
Before strike	102.3	4	148.4	2	218.6	5	310.1	2
Strike	–297.1	1	–460.1	2	–1,125.6	2	–1,027.4	2
After strike	184.1	5	365.6	2	681.4	5	702.3	3
Overall total	–10.7	10	53.9	6	–225.6	12	–15.0	7
% loss	0.1		–0.6		0.6		0.1	

SOURCES: U.S. Department of Commerce (various dates a); authors' calculations.

NOTES: Values represent the difference between the forecast level of imports under a no-strike scenario as specified by a vector autoregression equation and the actual goods imports. Figures are nominal seasonally adjusted values in millions of dollars. M is the number of months measured before, during, and after port closures.

from the forecast amount in the "but-for-no-strike" scenario.[5] In 1969, for example, there were excess imports totaling $219 million during the five months before the port closures. During the event, lost imports totaled $1.125 billion over two months—a loss of about 20 percent of total imports. In the three months following the closure, an additional $681 million worth of imports was brought in. Overall, the total loss of imports during the 10-month period was $226 million, or 0.6 percent of imports brought in during that period of time—a considerably smaller loss than what might initially be expected by looking at the shutdown period only. The estimated losses for the 1965 shutdown were of the same magnitude, and there appears to have been no lost trade at all in 1962 or 1971.

It is also worth noting that most of the adjustment in trade occurred after the shutdown, not before. Most firms dealt with the problem by making up for it with extra imports after the shutdown ended. Indeed, the run-up in imports ahead of the strike was on average slightly less than

[5]Why the number of months may vary from incident to incident would likely have to do with factors such as when the potential for a port strike was first recognized, how long the strike actually lasted, how rapidly the ports were up and running after the strike ended, as well as what types of goods flows were disrupted.

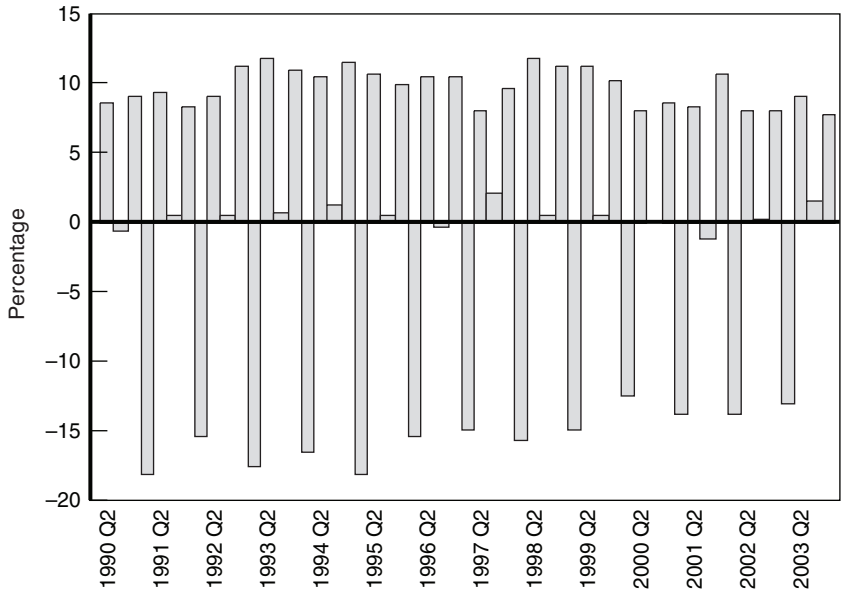
a third of the total reduction of trade during the strike. This small anticipatory response suggests either that most firms naturally carried enough essential retail or manufacturing inventory to get through a short-lived strike or that they had other sources.

Indeed, with these results in mind, it is hardly surprising then that we could find little evidence of the port shutdowns within the context of the broader economy. The statistical results reconfirm our eyeball results for the other four variables studied—manufacturing production; consumer spending on durable and non-durable goods; and employment in manufacturing, wholesale trade, and transportation. Very few of the strike indicator variables have any statistical significance, implying that there is little reason to believe that the strikes had any significant effect on the wider economy.

Summary and Conclusions

"Surely you must be joking!" might be the immediate response to the conclusion that a significant closure of the ports would have at most a mild effect on the economy. It would seem more likely that a substantial disruption to the supply chain because of a port shutdown would have a very dramatic effect on the production process. Yet all the evidence points to the opposite conclusion. The major labor actions of the sixties had measurable effects on the timing of imports but hardly any on total imports, and there is little or no evidence to support the idea that they had any substantial effect on the overall economy as measured by rising prices, falling employment, or a reduction in production activity.

The shutdowns did not have much of an effect for two reasons. One is that businesses deal every day with fluctuations in supply, demand, and production, as a result of both predictable seasonal variation and random events. It often is forgotten, in our world of seasonally adjusted statistics, just how much fluctuation there is in demand through the course of the year. Figure 2.10 shows the unadjusted quarterly patterns of growth in consumer spending on goods; a sizable negative is notable in the first quarter. Firms are quite able to deal with that strong seasonal variation through seasonal inventory, maintenance, and personnel policies. A disturbance to the flow of goods through a port is certainly



SOURCE: U.S. Department of Commerce (2006b).
NOTE: Data not seasonally adjusted.

Figure 2.10—Quarterly Changes in Real Consumer Spending on Goods

a large disturbance to the supply chain, but it must be remembered that it causes business to be delayed, not cancelled. A car or piece of furniture not purchased today because of a lack of available inventory will likely be purchased tomorrow. And firms do not lay off workers for temporary disruptions in demand or supply. Recession-causing events, such as a collapse of an information technology (IT) spending bubble, are long term, usually as long as a year. If the United States had its ports closed or had substantially reduced throughput for six months or more, then our analysis would surely be different.

This leads to the second reason why the shutdowns did not have much of an effect: Businesses and consumers are adaptable. When faced with the inability to bring a product through a port, a business will work to find another supply source—by importing from a different place, using a different mode of transport, or finding a domestic substitute. Consumers are similarly adaptable. If they cannot buy one product or

service because of a temporary shortage, they will buy different products and goods or simply wait a month until the product they want becomes available again.

Another difference between a recession-causing event, such as the bursting of the tech bubble, and a non-recession-causing event, such as a port shutdown or natural disaster, is that a recession-causing event is long-term (several quarters) and features a substantial (2% of GDP) drop in aggregate demand. A disaster or strike is too short-lived, too small, and comes with offsetting increases in demand for other goods and services. And there are domestic substitutes available.

Although the United States employs fewer people in manufacturing today than it did in 1965, the nation has a manufacturing productive capacity of three times the level of 40 years ago. Most of these jobs have been replaced with capital—not outsourced to China. And land neighbors Mexico and Canada also have capacity for the United States to tap into in times of need.

This is not to say that a port closure will have no economic effect. The increased transaction costs for businesses and consumers are certainly relevant, but of course these are too small to be evident in national statistics. And it is certainly true that some businesses will be hurt. Offsetting this is the fact that other businesses will benefit from a port closure because of the increased demand for their products. Some locations might also be adversely affected. Los Angeles may find itself suffering from a lack of throughput at the local ports. It must be remembered that workers are not laid off for business delayed—only for business cancelled. The local economy would suffer from a port closure of two months but there would be no significant loss of jobs, as we showed above in our discussion of the effect of the September 11 attacks and of natural disasters. The loss of a major industry—such as aerospace—would be far more threatening to the health of the local economy. And at the national level, some places and some industries will certainly be winners.

What lesson can be gleaned from this study? What can be done to reduce the effects of a terror-caused port shutdown? Since the potential damage to the U.S. economy from a relatively short port slowdown (say 10 to 30 days) would be relatively small, the government should assess

the benefits from port security in terms of the direct damage to lives and property that an attack might cause. Assessed that way, there may be other more critical issues such as bioterrorism or a dirty bomb attack within a dense residential neighborhood. To this end, greater port security might be needed, but the focus should be more on preventing the use of ports as a conduit for bringing potential weapons into the United States than on protecting a port itself from attack.

At the very least, the government should be careful not to impose draconian rules that limit the ability of the economy to adjust to the short-term shock. After the September 11 attacks, the government closed down commercial aviation for four days. If a similar reaction took place after an attack on the ports, the government itself might do more damage to the economy than the actual incident did.

Careful planning and preparatory steps now will help to keep secondary economic effects to a minimum. From port shutdown data, we infer that disruptions that last less than two months are not likely to cause serious secondary economic damage. We need plans and preparations to make sure that the duration of disruption is short. In terms of preparation, one possibility is to educate businesses that rely on imports through the port about the degree of their vulnerability and urge them to prepare by adding inventory. An ongoing assessment of the levels of critical inventories would be useful to them. Firms should also be encouraged to make plans for dealing with a short-run supply-chain disruption. The 2002 lockout may have already encouraged businesses to take these steps, but certainly the government should also have some role in continuing the planning process.

The government should also have a distinct plan of action to deal with the consequences of an attack. This would include developing a simple way to sort safe incoming cargo from risky incoming cargo—perhaps through identification of its place of origin—and to deal efficiently with the containers in the latter category. Such a plan would also include ways to prioritize imports. Not all imports are created equal. Some are more important than others and those firms using the more important imports have responded to past disturbances by working to bring in extra imports ahead of time. These same firms should get priority for entering the country. A government-run program for

making selections may not be the ideal. Rather, the market could decide through some sort of bidding mechanism, either directly, with the revenue going to the government, or indirectly, by having a lottery and then allowing firms to trade their "place in line" with other firms.

Appendix

This section details the regressions used to statistically test for significant effects of the port shutdowns. Shutdown indicator variables need to be chosen to distinguish anticipatory responses, concurrent effects, and ripple effects after the event. A number of months before and after the strike events were initially included, and dummy variables on either end that were statistically insignificant (with t-statistic of less than 1) were dropped from the equation. The same set of dummy variables was then included in a set of regressions for manufacturing production; consumer purchases of durable and non-durable goods; and total employment in manufacturing, wholesale trade, and transportation. The results of these regressions are included in Table 2A.1.

Consider first the imports regression. There did indeed seem to be an increase in imports before past port shutdowns. However, the amount of excess imports that occur is very small relative to the declines seen during the actual shutdown and seemed to occur many months ahead of time. For example, there was an unexpected 7.5 percent increase in imports in September 1962, three months before the strike began, as indicated by the positive and significant coefficient on the dummy variable for this month in our regression for imports. This is so much earlier than the strike because the strike actually began in late September or early October and ended within three days through presidential action under the authority of the Taft-Hartley Act. The strike began immediately after the 80-day waiting period was up in December. When this occurred, there was an "unexpected" decrease in imports of about 33 percent. Clearly, this is simply not enough to fully mitigate any potential losses that might be caused by the disruption to the supply chains.

A second point is that there were excessive levels of imports between one and four months after the strike ended as well. It is clear that the

Table 2A.1

Economic Performance Regressions with Strike Control Dummy Variables

Imports			Manufacturing Production			Payroll			Durables			Non-Durables		
R^2	0.998		R^2	0.999		R^2	0.999		R^2	0.995		R^2	0.998	
Adj. R^2	0.998		Adj. R^2	0.999		Adj. R^2	0.999		Adj. R^2	0.994		Adj. R^2	0.998	
DW stat.	1.922		DW stat.	2.020		DW stat.	2.322		DW stat.	2.164		DW stat.	1.890	
	Coef.	t-stat.		Coef.	t-stat.		Coef.	t-stat.		Coef.	t-stat.		Coef.	t-stat.
C	–6.212	–2.75*	C	–1.189	–2.34*	C	0.127	0.93	C	–0.375	–2.37*	C	0.684	1.66
Imports –1	0.529	9.76*	Product M –1	0.962	13.18*	Payroll T –1	0.831	19.42*	Durables –1	0.977	13.25*	Non-Durables –1	0.475	6.78*
Imports –3	0.264	5.29*	Product M –2	–0.200	–2.19*	Payroll T –2	0.160	2.45*	Durables –2	–0.327	–4.00*	Non-Durables –2	0.184	2.37*
Prices	0.926	1.72*	Product M –3	0.173	3.22*	Payroll O	0.492	4.24*	Durables –4	0.232	4.07*	Non-Durables –3	0.260	3.61*
Prices –1	–1.335	–1.74*	Inventories –3	–0.231	–3.45*	Payroll O –1	–0.224	–1.66*	Unemp –2	–0.033	–3.14*	Income –1	0.139	1.13
Prices –2	0.908	1.68*	Inventories –5	0.220	3.22*	Payroll O –3	–0.274	–2.66*	Unemp –3	0.025	2.45*	Income –2	–0.163	–1.32
Payroll	2.286	2.04*	Payroll	2.958	13.04*	Production	0.243	10.45*	Income –1	0.686	2.42*	Services	0.545	3.61*
Payroll –1	–2.692	–1.62	Payroll –1	–1.915	–5.31*	Production –1	–0.184	–5.53*	Income –4	–0.564	–2.04*	Services –2	–0.416	–2.67*
Payroll –2	4.475	2.68*	Payroll –2	–0.903	–3.15*	Production –3	–0.052	–2.61*	T–Bill –1	–0.013	–2.35*	Payroll	0.571	2.62*
Payroll –3	–3.518	–3.05*							T–Bill –2	0.011	1.42	Payroll –1	–0.631	–3.08*
Durables	0.212	2.11*							T–Bill –3	–0.008	–1.33			
Durables –1	–0.232	–2.15*												
Production –3	0.886	2.92*												
Production –4	–0.880	–3.08*												
Oil –1	0.077	2.89*												
Oil –8	–0.115	–4.92*												

Table 2A.1 (continued)

Dummy variables

Imports			Manufacturing Production			Payroll			Durables			Non-Durables		
	Coef	t-stat.		Coef	t-stat.		Coef	t-stat		Coef	t-stat		Coef	t-stat
Sep-62	0.074	2.10*	Sep-62	0.004	0.60	Sep-62	0.000	0.11	Sep-62	0.010	0.41	Sep-62	0.010	1.42
Oct-62	–0.070	–1.98*	Oct-62	–0.004	–0.54	Oct-62	0.000	0.09	Oct-62	–0.031	–1.26	Oct-62	–0.008	–1.14
Nov-62	0.036	1.00	Nov-62	0.012	1.56	Nov-62	–0.003	–0.92	Nov-62	0.055	2.23*	Nov-62	0.001	0.08
Dec-62	–0.039	–1.12	Dec-62	0.006	0.84	Dec-62	0.001	0.47	Dec-62	0.010	0.41	Dec-62	–0.002	–0.30
Jan-63	–0.222	–6.31*	Jan-63	0.008	1.02	Jan-63	–0.002	–0.61	Jan-63	0.002	0.10	Jan-63	0.002	0.24
Feb-63	0.211	5.62*	Feb-63	0.004	0.56	Feb-63	0.001	0.17	Feb-63	–0.006	–0.23	Feb-63	–0.009	–1.18
Nov-64	0.054	1.50	Nov-64	0.016	2.03*	Nov-64	0.005	1.69*	Nov-64	–0.048	–1.93*	Nov-64	–0.023	–3.14*
Dec-64	0.027	0.75	Dec-64	0.004	0.56	Dec-64	0.000	–0.06	Dec-64	–0.023	–0.94	Dec-64	0.010	1.41
Jan-65	–0.319	–8.84*	Jan-65	0.014	1.81*	Jan-65	–0.003	–0.87	Jan-65	0.028	1.14	Jan-65	–0.002	–0.30
Feb-65	0.085	2.11*	Feb-65	0.006	0.76	Feb-65	0.000	0.04	Feb-65	0.047	1.86*	Feb-65	0.009	1.16
Mar-65	0.110	3.10*	Mar-65	0.009	1.24	Mar-65	–0.001	–0.24	Mar-65	0.050	1.99*	Mar-65	–0.017	–2.33*
Apr-65	0.087	2.15*	Apr-65	–0.001	–0.12	Apr-65	0.002	0.56	Apr-65	0.026	1.01	Apr-65	0.003	0.40
Oct-68	–0.051	–1.46	Oct-68	0.000	–0.02	Oct-68	0.000	0.09	Oct-68	–0.004	–0.15	Oct-68	–0.007	–0.90
Nov-68	0.019	0.54	Nov-68	0.005	0.67	Nov-68	–0.001	–0.45	Nov-68	–0.020	–0.83	Nov-68	0.005	0.76
Dec-68	–0.015	–0.42	Dec-68	–0.007	–0.93	Dec-68	0.000	0.00	Dec-68	0.001	0.05	Dec-68	–0.012	–1.70*
Jan-69	–0.381	–10.94*	Jan-69	0.002	0.29	Jan-69	–0.003	–0.93	Jan-69	0.018	0.75	Jan-69	0.004	0.49
Feb-69	0.086	2.12*	Feb-69	–0.001	–0.10	Feb-69	0.001	0.19	Feb-69	0.001	0.04	Feb-69	0.005	0.72
Mar-69	0.052	1.47	Mar-69	0.002	0.27	Mar-69	–0.001	–0.17	Mar-69	–0.015	–0.62	Mar-69	0.002	0.21
Apr-69	0.140	3.56*	Apr-69	–0.006	–0.86	Apr-69	0.001	0.46	Apr-69	0.018	0.71	Apr-69	0.003	0.35
May-69	0.048	1.35	May-69	–0.010	–1.32	May-69	0.001	0.48	May-69	–0.007	–0.30	May-69	0.002	0.34
May-71	0.043	1.24	May-71	–0.005	–0.68	May-71	0.002	0.66	May-71	–0.012	–0.49	May-71	–0.006	–0.78
Jun-71	0.044	1.26	Jun-71	0.000	–0.03	Jun-71	–0.006	–2.08*	Jun-71	0.018	0.73	Jun-71	0.005	0.75

Table 2A.1 (continued)

Dummy variables

Imports			Manufacturing Production			Payroll			Durables			Non-Durables		
	Coef.	t-stat.		Coef.	t-stat.		Coef.	t-stat.		Coef.	t-stat.		Coef.	t-stat.
Jul-71	–0.032	–0.89	Jul-71	0.000	0.03	Jul-71	0.000	0.01	Jul-71	–0.046	–1.82*	Jul-71	–0.009	–1.20
Aug-71	0.002	0.06	Aug-71	–0.014	–1.85*	Aug-71	0.002	0.58	Aug-71	0.021	0.83	Aug-71	0.001	0.15
Sep-71	0.046	1.30	Sep-71	0.008	1.10	Sep-71	–0.001	–0.26	Sep-71	0.045	1.82*	Sep-71	–0.007	–0.91
Oct-71	–0.141	–3.92*	Oct-71	0.007	0.88	Oct-71	–0.004	–1.23	Oct-71	0.009	0.35	Oct-71	–0.006	–0.82
Nov-71	–0.069	–1.91*	Nov-71	–0.002	–0.25	Nov-71	0.000	0.09	Nov-71	0.014	0.55	Nov-71	0.003	0.44
Dec-71	0.091	2.46*	Dec-71	–0.001	–0.15	Dec-71	–0.001	–0.46	Dec-71	–0.002	–0.07	Dec-71	–0.002	–0.31
Jan-72	0.102	2.85*	Jan-72	0.010	1.34	Jan-72	–0.007	–2.36*	Jan-72	0.020	0.80	Jan-72	–0.017	–2.39*
Feb-72	0.073	1.98*	Feb-72	–0.003	–0.41	Feb-72	–0.001	–0.35	Feb-72	–0.037	–1.48	Feb-72	–0.004	–0.50

NOTES: All variables seasonally adjusted, log form. Sample period 1959 to 1976. Definition of terms: imports—goods imports (Census); prices—producer price index; payroll—total non-farm payroll employment; payroll t—payroll employment in manufacturing, transportation, and wholesale; payroll o—payroll employment in everything else; income—personal income; durables—real consumer spending on durables; non-durables—real consumer spending on non-durables; services—real consumer spending on services; production—industrial production; product m—industrial production in manufacturing; inventories—manufacturing inventories; unemployment—unemployment rate; t-bill—interest rate on three-month Treasury Bill; DW stat.—the Durbin-Watson statistic. Strike and labor-related shutdown periods are shaded.

*Indicates variables significant at the 10 percent level.

decline in imports during the strike did not represent the total loss of imports—in many cases the strike simply delayed shipments rather than cancelling them. As pointed out before, delayed business does not have a large effect on the overall economy, only cancelled business does.

Because of the dynamic responses embedded in the model, the dummy variables cannot simply be totaled up to calculate the permanent loss in trade. Instead a simulation can be run where the strikes are in effect removed, by setting the dummy variables equal to zero and predicting imports through the strike periods as if the strike had not occurred. The difference between the forecast values with the dummy variables turned on and the predicted values with the dummy variables turned off is our best estimate of the total reduction in trade through the relevant time periods. A valid criticism of this technique might be that industrial production and consumer spending on durables and non-durables are not exogenous to imports, and thus this method will underestimate the true degree of lost imports. Thus, a second method, vector autoregression, is used with the other specified equations in order to allow all variables to be different in the no-strike scenario.

References

"American Flag Is a Hot Item Today, But Consumers May Cut Spending" (a *Wall Street Journal* News Roundup), *Wall Street Journal*, September 13, 2001, p. B6.

"Costs Mount Rapidly in Dock Strike As Some Pact Talks Remain Stalled" (a *Wall Street Journal* News Roundup), *Wall Street Journal*, February 9, 1965, p. 30.

"Dock Strike Losses in Revenues and Wages Put at $400 Million; Ships Jam Harbors" (a *Wall Street Journal* News Roundup), *Wall Street Journal*, January 8, 1963, p. 4.

Federal Reserve Bank of St. Louis, "Archival Federal Reserve Economic Data (ALFRED): Manufacturing Sector Output (1996 Vintage Data)," St. Louis, Missouri, August 5, 1999, available at research.stlouisfed.org/fred2/series/OUTMS/ (as of February 16, 2006).

Gaudette, Karen, "Court Approves Bush Request to Open West Coast Ports," the Associated Press State and Local Wire, 2002.

Martin Associates, *The Potential Impact of Trucker Demand and Supply Issues at U.S. East Coast and Gulf Coast Ports,* Lancaster, Pennsylvania, 2005.

"Paralyzed Piers: Impact of 21-Day Dock Strike Is Spreading; Costs Incurred Seen Leading to Price Rises" (a *Wall Street Journal* News Roundup), *Wall Street Journal*, January 9, 1969, p. 34.

Thornberg, Christopher, "The Economic Effect of the September 11th Attacks: A One-Year Retrospective," *The UCLA Anderson Forecast for the Nation and California,* September 2002.

U.S. Department of Commerce, Bureau of the Census, Foreign Trade Division, "U.S. Imports and Exports of Merchandise," Washington, D.C., various dates a.

U.S. Department of Commerce, Bureau of the Census, *Statistical Abstract of the United States*, Washington, D.C., various dates b, available at www.census.gov/prod/www/abs/statab.html (as of February 21, 2006).

U.S. Department of Commerce, Bureau of the Census, Retail Indicators Branch, "Monthly Retail Trade Survey," Washington, D.C., February 14, 2001, available at www.census.gov/mrts/www/mrts.htm (as of February 21, 2006).

U.S. Department of Commerce, Bureau of Economic Analysis, "Trade in Goods and Services (Census Basis)," Washington, D.C., June 10, 2005a, available at www.bea.gov/bea/di/home/trade.htm (as of February 16, 2006).

U.S. Department of Commerce, Bureau of Economic Analysis, "State Quarterly Income Estimates," Washington, D.C., December 20, 2005b, available at www.bea.gov/bea/regional/statelocal.htm (as of February 16, 2006).

U.S. Department of Commerce, Bureau of Economic Analysis, "Current-Dollar and Real Gross Domestic Product," Washington, D.C., January 27, 2006a, available at www.bea.gov/bea/dn/home/gdp.htm (as of February 16, 2006).

U.S. Department of Commerce, Bureau of Economic Analysis, "Personal Income and Outlays," Washington, D.C., January 30, 2006b, available at www.bea.gov/bea/dn/home/personalincome.htm (as of February 16, 2006).

U.S. Department of Commerce, Bureau of the Census, Manufacturing and Construction Division, "Manufacturers' Shipments,

Inventories, and Orders, SIC Based Historic Statistics," Washington, D.C., February 3, 2006c, available at www.census.gov/indicator/www/m3/hist/m3bendoc.htm (as of February 21, 2006).

U.S. Department of Commerce, Bureau of the Census, Retail Indicators Branch, "Monthly Wholesale Trade Survey," Washington, D.C., February 9, 2006d, available at www.census.gov/svsd/www/mwts.html (as of February 21, 2006).

U.S. Department of Labor, Bureau of Labor Statistics, "Current Employment Statistics," Washington, D.C., n.d.a, available at www.bls.gov/ces/home.htm (as of February 16, 2006).

U.S. Department of Labor, Bureau of Labor Statistics, "Producer Price Indexes," Washington, D.C., n.d.b., available at www.bls.gov/ppi/home.htm (as of February 16, 2006).

U.S. Department of Labor, Bureau of Labor Statistics, "Current Employment Statistics: Discontinued CES Data on SIC," Washington, D.C., June, 6, 2003, available at www.bls.gov/ces/cesoldsic.htm (as of February 21, 2006).

U.S. Department of State, Bureau of Public Affairs, Office of the Historian, "Significant Terrorist Incidents, 1961–2003: A Brief Chronology," Washington D.C., March 2004, available at www.state.gov/r/pa/ho/pubs/fs/5902.htm (as of February 16, 2006).

U.S. Department of Transportation, Maritime Administration, "U.S. Waterborne Foreign Trade Statistics: U.S. Waterborne Trade by U.S. Custom Ports, 1997–2004," Washington, D.C., n.d., available at www.marad.dot.gov/MARAD_statistics/index.html (as of February 21, 2006).

3. The Costs of a Terrorist Attack on Terminal Island at the Twin Ports of Los Angeles and Long Beach

Peter Gordon, James E. Moore, II, and Harry W. Richardson
University of Southern California

Qisheng Pan
Texas Southern University, Houston

Introduction

According to recent estimates, almost $30 billion was spent or budgeted by federal agencies in the period 2001–2005 to protect the U.S. homeland from terrorist attack.[1] What is the best use of these resources? How can we improve on current allocations? These are not simple questions, but a growing body of research, some funded by the U.S. Department of Homeland Security (DHS), is beginning to address their various aspects.

One approach to this question of cost-effectiveness is to estimate the economic losses from various hypothetical attacks and then identify the reductions in losses from various mitigating measures. We did this in a previous analysis, which hypothesized the effects of simultaneous radiological bomb attacks on the Los Angeles and Long Beach ports.[2] These ports account for a substantial share of local economic activity—more than 600,000 jobs and $250 billion of import and export trade.

[1] Brunet (2004).

[2] Gordon et al. (2005a).

This study is part of a research program to apply the Southern California Planning Model (SCPM) and similar economic impact models to estimate the economic losses from hypothetical but plausible terrorist attacks on various key infrastructure installations and other important sites.

In this chapter, we explore another dimension of potential terrorist attacks on the region's ports. Terminal Island, a zone of concentrated container activity in the port complex, shown in the port map on p. xxiii, accounts for about 55 percent of the twin ports' trade, and it could easily be isolated by destroying three highway bridges and one rail bridge. We assume four simultaneous conventional bomb attacks on these bridges of a size sufficient to destroy them. We then estimate the potential economic losses associated with the closure of Terminal Island.

One major difficulty with this approach is estimating a reasonable "back to business" recovery period. At the low end, one or more friction pile bridges could be built within three or four months. Such bridges have their own problems, however: They would be close to sea level and built on caissons embedded into the seabed and so would probably interfere with shipping lanes. A bridge would also have to be built for trains carrying containers to and from Terminal Island—a project that would create a different set of problems.

At the other end of the timeline, two years would permit the total rebuilding of the bridges on their original scale, but even this would be optimistic given institutional rather than reconstruction constraints. Because the model is linear, any chosen time period could easily be adjusted and, below, we suggest how the problems created by linearity might be addressed. As we will show, the one-year economic cost is $45 billion, split about two-thirds outside the region and one–third within. The range of effects is between $15 billion and $90 billion. Although estimating how long it would take to reopen Terminal Island and with what level (and degree of permanence) of infrastructure access is somewhat speculative, there is no doubt that a simultaneous four-bridge attack would be a significant and costly event that would fully merit substantial resource expenditures to prevent. Similarly, if an attack were to occur, there would be substantial cost savings derived from efforts to accelerate the reopening date.

The Los Angeles and Long Beach Ports

The Los Angeles/Long Beach ports' role in the local and national economy is widely recognized. The port complex stands in a metropolitan region of more than 16.4 million people with a labor force of almost 7.5 million and a median annual household income of $46,000; the twin ports account for 111 million tons of seaborne trade each year and constitute the fifth-largest port complex in the world after Hong Kong, Singapore, Shanghai, and Shenzhen. Directly and indirectly, the ports employ 600,000 workers, accounting for more than 7 percent of the region's labor force. In terms of containerized traffic passing through, the two ports rank first and second nationally.

To put this in perspective, their combined import and export trade flow of $250 billion in 2004 is equivalent to about 30 percent of the greater Los Angeles gross regional product. Reflecting trends in the national economy, imports are about five times larger than exports. About one-half of the imports and two-thirds of the exports are to and from areas beyond the Los Angeles region. The ports fill a national more than regional function. The loss of transshipment capabilities at these sites would have profound effects both locally and nationally.

Any major disruption of port activities would have effects beyond the disruption of international trade flows, the short-term inability of consumers to buy imported goods, or deferred export sales by producers. The supply chains for imported raw materials and intermediate inputs would also be disconnected, thus reducing the productive capacity of firms both inside and outside the region. The problem would be exacerbated by low inventories associated with a widespread shift to the usually more efficient just-in-time inventory system.

We assume that both export and import flows currently using local seaport facilities would terminate for as long as the ports were out of service. We have not yet modeled port diversion but may do so in future research, probably beginning with a survey of fleet operators. Some observers have suggested focusing on the experience provided by the West Coast lockout of 2002, when ships bound for Los Angeles–Long Beach diverted to other ports, but this incident is of limited relevance because the closure was widely anticipated and the loss estimates

suggested at the time ($1 billion each day) were wildly inaccurate. This figure was cited widely in many media outlets, but the original source for it remains unknown. However, this figure is about three-and-a-half times our upper-bound estimate of the cost of a closure of Terminal Island—even after accounting for multiplier effects. During the 2002 port closure, some carriers substituted access to the Gulf Coast for service at local ports. Container flows through the Panama Canal also increased. But this would not be a viable alternative for a terrorist attack scenario, because approximately half of all Pacific cargo ships are of post-Panamax design, meaning that they are too large to fit through the Panama Canal. Other Pacific ports do not have the draft, or depth of channel, or enough cranes to absorb the current traffic moving through the ports of Los Angeles and Long Beach. The extent and duration of diversions resulting from the unscheduled closure of local ports remain difficult to predict. Although larger ships, capable of carrying more than 8,000 20-foot equivalent units (TEUs) of containers have been put into service, their only alternative West Coast destination is Seattle-Tacoma.

Although the 2002 experience might not be the best example, port diversion remains one of many mitigation strategies that might be adopted to alleviate the effects of bomb attacks on the twin ports. Such mitigation measures imply that our estimates of economic effects are probably upper bounds. Some others are discussed below.

The Southern California Planning Model

Interindustry models based on the transaction flows between intermediate suppliers and end producers are widely used to measure regional economic effects. They trace all economic effects, including those of intra- and interregional shipments, usually at a high level of sectoral disaggregation. They are demand-driven and account for losses primarily via backward and forward linkages between economic sectors.

The input-output model component in this study is built on the Minnesota Planning Group's well-known IMPLAN model, which has a high degree of sectoral disaggregation (509 sectors), aggregated to 17 sectors for small-scale area effects.[3] The second basic model component

[3]IMPLAN is an acronym for Impact Analysis for Planning.

(which is spatial) allocates sectoral effects across 1,527 geographic zones throughout Southern California (encompassing the greater Southern California five-county region, including Los Angeles, Orange, Riverside, San Bernardino, and Ventura Counties). The key aspect of the model is the spatial allocation of indirect and induced effects generated by the input-output model. The direct effects consist of the final demand changes at the source of the attack (in this case, at the ports), the indirect effects trace the interindustry linkages with other sectors, either forward or backward (locally, regionally, nationally, and internationally), and the induced effects measure the secondary consumption effects associated with the reduced spending of workers in both the direct and indirect sectors. To estimate the latter, we use a journey-to-work matrix that shows all the commuting flows between residential zones and workplace zones to trace wages earned back to the home and then a journey-to-services matrix to trace retail and personal service purchases from the home to retail and service establishments. The journey-to-services matrix includes any trip associated with a home-based transaction other than the sale of labor to an employer. This includes retail trips and other transaction trips but excludes non-transaction-based trips such as those to visit friends and relatives. Data for the journey-to-services matrix include all trips classified by the Southern California Association of Governments (SCAG) as home-to-shop trips and a subset of the trips classified as home-to-other and other-to-other trips.

The current version of the Southern California Planning Model endogenizes traffic flows. It uses Traffic Analysis Zones (TAZs), which are very small geographical units appropriate for measuring traffic flows from one node to another. This extension is important, because many types of terrorist attacks are likely to induce changes in supply, including infrastructure capacity losses that will contribute to reductions in network-level service and to increases in travel delays. These delays and potential infrastructure damages are not negligible, but they are overwhelmed by the general effects of business interruption.

When traffic flows are endogenous, any change in economic activity that affects the travel behavior of individuals or the movement of freight will influence how the transportation network is used, and these effects will work themselves out as a change from one network equilibrium to

another. In an earlier paper, we accounted for the simultaneous losses of highway bridges and shipping facilities.[4] The scenario examined in this chapter is more focused and isolates Terminal Island via bridge losses. The model can estimate losses from concurrent attacks against shipping, infrastructure, and productive capacity.

Treating the transportation network explicitly endogenizes the otherwise exogenous travel behavior of households and intraregional freight flows, achieving consistency across network costs and origin-destination requirements. The model makes explicit distance decay (the decline in the number of trips with increasing distance) and congestion functions (the buildup of traffic congestion and delay costs as particular routes attract more traffic when other parts of the network are disrupted).

This allows us to determine the geographic location of indirect and induced economic losses by endogenizing route and destination choice. It also enables us to more accurately allocate indirect and induced economic losses over TAZs in response to port-related direct losses in trade, employment, and transportation accessibility.[5]

Radiological Bomb Attack Simulations

In previous research, we explored the effects of simultaneous radiological bomb attacks on the twin ports of Los Angeles and Long Beach. These could be either brought in by container or planted very close to the port perimeter, assuming that the terrorists have access to suitable radioactive material within the United States.

The extent of the disruption would depend on the size of the bombs. In our previous research, we assumed an explosion of two small radiological dispersal devices (RDDs), each containing five pounds of high explosive, more or less simultaneously at the two ports. We estimated blast damage to be modest, with deaths and serious injuries occurring only within a range of about 15 meters and with very limited damage to physical infrastructure. The evacuation zone would include all areas with exposure of greater than 1 REM (roentgen equivalent

---

[4]Gordon et al. (2005a).

[5]See Cho et al. (2001) for a detailed summary of an earlier version of this model.

man), probably within a range of five to 10 square kilometers, depending on weather conditions such as wind speed, wind direction, and precipitation. In a subsequent study, we are attempting to measure "plume effects" in terms of household disruption, business losses, and decline in real estate values. The numbers are very speculative, but our best estimate is a $4 billion loss in output and a decline of nearly 42,600 person-years of employment. Such an attack would require the closure of both ports for health rather than security reasons. The early phase of radiation exposure lasts about four days, according to Environmental Protection Agency (EPA) guidelines; the time frame for intermediate and later phases is variable and subjective and can be measured in weeks, months, and even years. When the ports might reopen would be a policy rather than a technical decision.

In the previous RDD scenario, we estimated that the closure of the Los Angeles and Long Beach ports for 15 to 120 days (for the latter case we combined the radiological bomb attacks with conventional bombs blowing up three key access bridges and overpasses) could cost the U.S. economy up to $34 billion—or more than 212,000 person-years of employment. Tables 3.1a and 3.1b show aggregate results and county-level detail. The model also provides economic results in much greater spatial detail, to the level of census tracts or traffic analysis zones if required.

We will not report in detail on the results shown in Tables 3.1a and 3.1b, because these are discussed at length elsewhere.[6] Nevertheless, a few comments are appropriate. These two widely different scenarios result in a wide range of economic effects—from $4.3 billion of lost output and 26,500 person-years of employment at the low end, to $34.1 billion of lost output and 212,200 person-years at the high end. Table 3.1a illustrates a minimum impact scenario, with the ports reopened quickly after 15 days—a policy decision, not a technical one, that would involve some degree of political risk. Table 3.1b combines the radiological bomb attack with the destruction of freeway access bridges and overpasses. Extrapolating from the accelerated rebuilding of a Santa

[6]Gordon et al. (2005a).

Table 3.1a

Output and Employment Losses from a 15-Day Closure of the Ports of Los Angeles and Long Beach

	Output ($ Millions)				Jobs (Person-Years)			
	Direct	Indirect	Induced	Total	Direct	Indirect	Induced	Total
City of Los Angeles	264	94	65	423	1,186	724	729	2,639
City of Long Beach	69	12	7	88	502	80	75	657
Los Angeles County	657	220	157	1,034	3,091	1,654	1,768	6,513
Orange County	156	62	45	262	688	480	501	1,669
Ventura County	43	18	12	73	182	121	131	435
Riverside County	37	14	13	64	163	111	147	421
San Bernardino County	53	20	16	89	230	152	186	568
Sum of five counties	946	334	243	1,522	4,354	2,519	2,733	9,606
Out of region	1,782	515	440	2,736	8,050	3,907	4,957	16,914
Total	2,728	849	683	4,259	12,404	6,427	7,690	26,521

NOTE: Columns and rows may not sum to totals because of rounding.

Table 3.1b

Output and Employment Losses from a 120-Day Closure of the Ports of Los Angeles and Long Beach

	Output ($ Millions)				Jobs (Person-Years)			
	Direct	Indirect	Induced	Total	Direct	Indirect	Induced	Total
City of Los Angeles	2,113	753	520	3,385	9,492	5,788	5,831	21,111
City of Long Beach	554	93	53	700	4,008	640	601	5,249
Los Angeles County	5,252	1,759	1,260	8,271	24,722	13,233	14,142	52,097
Orange County	1,247	496	357	2,100	5,502	3,841	4,009	13,352
Ventura County	345	143	93	581	1,459	971	1,052	3,482
Riverside County	296	115	102	513	1,306	890	1,175	3,371
San Bernardino County	424	161	129	715	1,842	1,218	1,487	4,548
Sum of five counties	7,564	2,674	1,941	12,179	34,831	20,154	21,865	76,850
Out of region	14,256	4,116	3,520	21,892	64,401	31,259	39,655	135,316
Total	21,820	6,791	5,461	34,071	99,232	51,413	61,520	212,165

NOTE: Columns and rows may not sum to totals because of rounding.

Monica Freeway overpass after the Northridge earthquake in 1994, it would take a minimum of 120 days to restore full access to the ports.

As for how losses are broken down geographically, we will defer that discussion until we examine the Terminal Island attack scenario, outlined below.

These earlier results are primarily presented for comparison with the Terminal Island scenario. Both are significant events. Our assessment, however, is that a Terminal Island attack would be much easier to carry out, and (under certain assumptions about the length of disruption) might be more devastating in terms of economic effects. However, it would not inflict the potentially more serious psychological damage associated with a more general radiological bomb attack on the port complex.

The 120-day estimates were based on scenarios in our earlier research that involve destruction of various access bridges, which significantly multiplies the downtime of the ports. The ports could reopen earlier and shippers could resort to congested surface streets but at a substantial efficiency cost. Thus, an additional $90 million dollars in transportation network delay costs are incurred in the 120-day scenario. This scenario includes a loss of network capacity in this period because of bridge damage and a reduction in transportation demand because of the ports' closure. The model estimates the associated changes in network flows and costs (Table 3.2). The results appear quite modest when expressed in percentage terms, but the absolute dollar amounts are far from negligible. Although the Terminal Island scenario is measured over a longer period, its proportionate effect is less than that of a radiological bomb attack, because the transportation network consequences are much more geographically constrained.

Terminal Island Attack Simulation

Researchers at the University of Southern California Center for Research and Economic Analysis of Terrorism Events (CREATE) have developed several approaches to the formation of plausible terrorist attack scenarios, such as the radiological bomb scenario. Our models make it possible to estimate the economic effects of these scenarios.

Table 3.2

Change in Transportation Network Delay Costs for Multiple Impact Scenarios

	$ Millions			Percent Change[a]		
	Freight Travel Costs[b]	Personal Travel Cost[c]	Total Costs	Freight Travel Costs	Personal Travel Cost	Total Costs
15-day radiological scenario	–25	–24	–49	–2.39	–0.49	–0.81
120-day radiological scenario	–117	207	90	–1.42	0.52	0.19
Terminal Island scenario—one year	–338	395	58	–1.34	0.32	0.04

NOTES: The table shows changes in the monetary value of transportation flows resulting from several different scenarios. These values can change as a result of less capacity on the transportation network, raising costs, and fewer trips on the network, lowering costs. The 15-day radiological scenario is a 15-day halt at the port complex because of an RDD attack. The 120-day radiological scenario is a 120-day halt at the port complex because of an RDD attack and closure of roads into the port complex. The Terminal Island scenario—one year involves the destruction of three road bridges and one railroad bridge into Terminal Island and a one-year closure of only that part of the port complex. Total cost values may not sum to totals because of rounding.

[a]Percentage changes are changes from what would be experienced under normal operating conditions. For example, the percentage change in freight travel costs for the 15-day radiological scenario is the percentage difference over a period of 15 days under normal conditions.

[b]Freight trip cost is assumed to be $35.00 per passenger car equivalent (PCE) per hour.

[c]Personal trip cost is assumed to be $13.00 per PCE per hour.

Because our previous work determined that many of the ports' vulnerabilities arise from restricted highway access to most of the docks, we decided to further study the implications of bridge attacks intended to isolate all or part of the port complex. In particular, freight going to and from Terminal Island now accounts for a significant portion of combined port activities. Port authorities were unable to provide exact figures (primarily because of the reluctance of each highly competitive

port to release data that would be available to the other), but the best estimate is 55 percent of total trade dollars.

The Terminal Island docks are accessed by three major highway bridges—the Vincent Thomas Bridge, the Gerald Desmond Bridge, and the Commodore Schuyler F. Heim Lift Bridge—and, parallel to the Heim Bridge, by a rail bridge (Badger Bridge), which handles 21 percent of Terminal Island trade (Table 3.3; see also the port map, p. xxiii). These bridges are all high enough to permit ship traffic in the waters between the coast and Terminal Island. The Desmond Bridge, for example, is 250 feet above the water, although some experts consider that it is still too low to facilitate problem-free movement.

Our current simulations revealed that an attack making these bridges inaccessible for 12 months would create economic losses of almost $45 billion per year, accounting for job losses of nearly 280,000 person-years.

As shown by the data in Table 3.4, the overall output multiplier—or total economic activity changes generated by initial changes in economic activity—is 1.564 ($44.9 billion ÷ $28.7 billion) and the corresponding job multiplier—or total employment changes generated by initial changes in employment—is 2.142 (280,000 ÷ 130,700). The local multipliers have different values (the city of Long Beach local multiplier is only 1.40 whereas the Orange County multiplier is 2.41). But the local multipliers are difficult to interpret in economic terms because indirect and induced effects freely spill over administrative boundaries, and we believe that terrorist attack consequences must be evaluated more in regional and national than in local terms. Indirect effects are more

Table 3.3

Highway and Rail Access Bridges to Terminal Island

Bridge	City	Year Built	Span (feet)
Vincent Thomas Bridge	Los Angeles	1964	6,500
Gerald Desmond Bridge	Long Beach	1968	5,134
Commodore Schuyler F. Heim Lift Bridge	Long Beach	1946	3,976
Badger Rail Bridge	Long Beach	1997	3,976

Table 3.4

Output and Employment Losses from a One-Year Closure of Terminal Island

	Output ($ Millions)				Jobs (Person-Years)			
	Direct	Indirect	Induced	Total	Direct	Indirect	Induced	Total
City of Los Angeles	2,848	1,001	687	4,537	13,087	7,708	7,707	28,503
City of Long Beach	621	123	70	815	4,143	851	792	5,787
Los Angeles County	6,907	2,342	1,664	10,914	32,213	17,629	18,692	68,535
Orange County	1,663	660	472	2,796	7,371	5,118	5,302	17,791
Ventura County	462	189	123	774	1,961	1,290	1,390	4,641
Riverside County	393	152	134	680	1,744	1,185	1,546	4,475
San Bernardino County	563	214	170	949	2,460	1,621	1,963	6,044
Sum of five counties	9,990	3,559	2,565	16,115	45,749	26,842	28,894	101,485
Out of region	18,686	5,441	4,625	28,754	84,920	41,445	52,116	178,482
Total	28,677	9,001	7,190	44,869	130,669	68,288	81,010	279,967

NOTE: Columns and rows may not sum to totals because of rounding.

important than induced effects in terms of output but less important in terms of jobs. This is easily explained by the labor intensity of retail trade that dominates the induced effects, whereas the suppliers of intermediate inputs tend to be capital-intensive.

The geographic distribution of effects is also shown in Table 3.4. About 65 percent of both output and job effects are experienced outside the region. Of the regional effects, 68 percent occur within Los Angeles County. The effects in the other counties are not negligible, especially in Orange County, whose northern portions are relatively close to the ports. Not surprisingly, within Los Angeles County, about one-half of the effects occurred in the two port cities, overwhelmingly in Los Angeles rather than in Long Beach. This was due in part because Los Angeles's large size captured high shares of the indirect (intermediate linkage) and induced (secondary consumption) effects and in part because the bulk of the facilities on Terminal Island are owned by the Port of Los Angeles, not the Port of Long Beach.

Figure 3.1 maps detailed spatial employment loss results for the region under the Terminal Island scenario. The map shows the absolute number of job losses in each TAZ throughout the region. The darker the shade, the larger the job loss. Note that job losses are not clustered around the ports but instead are widely dispersed throughout the region, because trade flow interruptions have more than highly localized effects. Unlike other applications of the model, the regional and national implications are probably more important than the local effects in this case. The fact that effects are so widely dispersed could be helpful for local governments seeking to show that they too should participate in any federal budget allocations that emphasize port security.

Table 3.2 compared changes in transportation costs across all three types of scenarios—the baseline scenarios, the RDD scenarios, and the Terminal Island scenario. In the case of the Terminal Island scenario, network costs increase by $58 million per year (obtained by subtracting the baseline one-year effect from the Terminal Island one-year effect). This represents only a 0.04 percent increase in travel delays. There would be substantial reductions in freight travel costs because many port-related trucks are not on the road, but these would be offset by increased personal travel delays attributable to the absence of the Vincent Thomas Bridge linking harbor-area cities to Long Beach. This $58 million value is lower than the increase in delay costs associated with the 120-day RDD scenario because the Terminal Island scenario represents only a partial elimination of port capacity. These are delay costs only and do not include estimates of bridge repair costs.

It is difficult to determine how quickly access to Terminal Island could be restored. Our approach can be used to approximate the benefits of repairs faster than the normal two years, including the installation of temporary facilities. High-capacity temporary bridges might be constructed relatively quickly, but their design would place them close to the water, blocking ship traffic in the channels.

Table 3.5 scales the total losses for the Terminal Island scenario by six-month increments up to two years. The annual loss is equivalent to about 6 percent of gross regional product and about 3.7 percent of regional jobs. Also, as mentioned above, 64 to 65 percent of these losses occur in the rest of the United States, not within the region. The

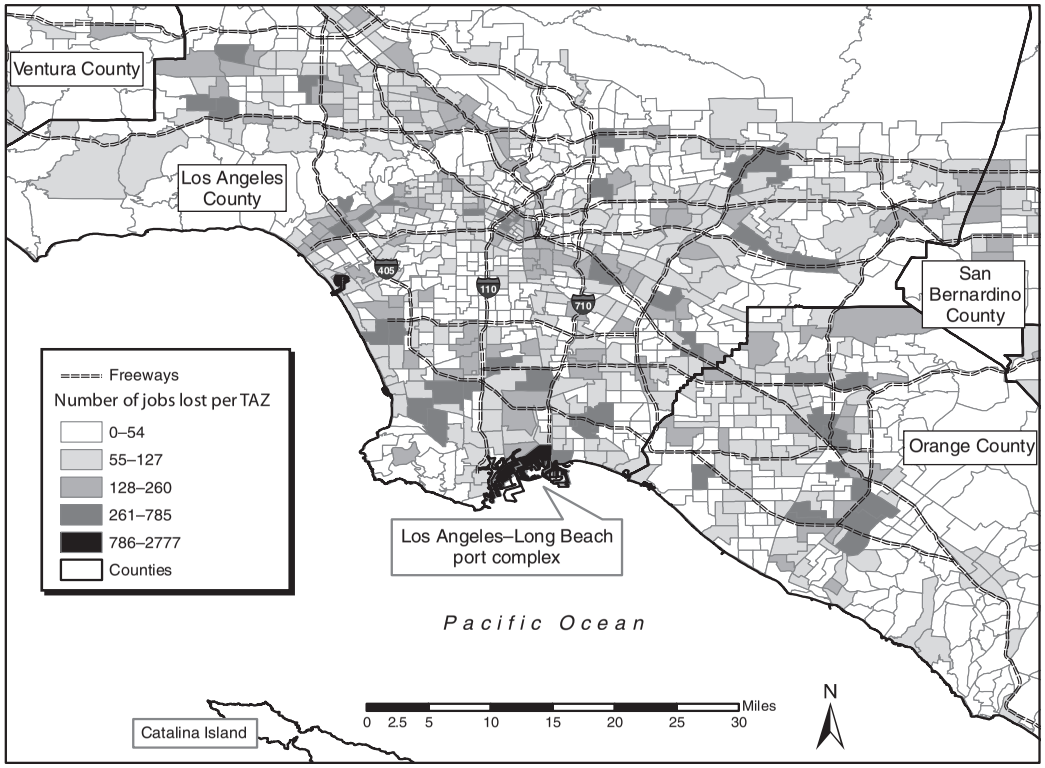


Figure 3.1—Spatial Distribution of Job Losses from a One-Year Closure of Terminal Island

Table 3.5

Total Output and Highway Network Losses for Alternative Bridge Reconstruction Periods

Length of Bridge Loss	Output Loss ($ Millions)	Network Loss ($ Millions)	Total Loss ($ Millions)
24 months	89,700	115.8	89,900
18 months	67,300	86.9	67,400
12 months	44,900	57.9	44,900
6 months	22,400	29.9	22,500

NOTE: Rows may not sum to totals because of rounding.

benefits of accelerated repairs are approximated by the differences between Row 1 of Table 3.5 and the row corresponding to the actual repair period. The differences are quite large. The implications are obvious: It is highly cost-effective to analyze emergency bridge reconstruction options and put into place plans for the protection of the Terminal Island access routes or their speedy replacement.

The San Francisco–Oakland Bay Bridge carries 275,000 passenger car equivalents each day, approximating the scale of the Vincent Thomas Bridge. The California Department of Transportation estimates the costs of the Bay Bridge replacement span at more than $6 billion. The other bridges now serving Terminal Island are comparatively smaller and would be cheaper to replace. Assuming a $12 billion total reconstruction cost for all bridges is conservative but plausible. It is unknown to what extent these costs might rise if construction were accelerated. Accepting the linearity assumptions associated with our alternative loss estimates, accelerating access to all three bridges would have an economic benefit of $3.75 billion per month.

Planning now to protect these facilities or for reconstruction or rapid temporary replacement of these critical bridges requires little, if any, deliberation. The costs of accelerated repairs to the Santa Monica Freeway bridges following the Northridge earthquake were easily justified. Our modeling approach makes it possible to be specific ex ante about the efficiency gains of accelerated repairs.

Qualifications and Comparisons

Standard objections to the use of models of this type are the linearity assumptions and the treatment of consequences as a single event. Proponents of these counterarguments contend that costs are likely to follow a non-linear path, perhaps rising incrementally after a few days (see Stephen S. Cohen, Chapter 4), then falling over time as behavioral adjustments are made. Although in the presentation of results we posit finite closures followed by full-scale reopening, the model can be adapted to non-linear time paths by decomposing the time frame into a set of linear phases of different dimensions that, when combined, simulate a non-linear path. Indeed, in a study of terrorist attacks on American theme parks, we used the model in non-linear fashion with periods of closure, followed by operation at a low capacity, and then a gradual return to pre-attack levels of activity over an 18-month period.[7]

As yet, there is considerable uncertainty about the length of time that Terminal Island might be unavailable. The two-year estimate, with its $90 billion of economic losses, might be an overestimate for several reasons. Although there may be some potential for diversion of ships to other ports, especially in the longer run, the evidence suggests that this is a limited option, primarily because of the restricted ability of other West Coast ports (except for Seattle-Tacoma) to accommodate the new container ships that account for an increasing proportion of total trade.

The construction of temporary bridges on grounded pillars would certainly accelerate truck access to Terminal Island, probably to within a three- to four-month range, but a temporary rail bridge would be more problematic. Overall, the costs in terms of disruption to the shipping lanes are difficult to determine and remain an issue for further study.

The database for the model dates from 2001, primarily dictated by the lag in U.S. Commodity Flow Survey (CFS) data. Because there has been a significant growth in trade since then, economic effects using an updated model with 2004–2005 data would be even larger than those derived here.

---

[7] Gordon et al. (2005b).

Another objection is that the methodology ignores the fine details of supply chain logistics. This study is about modeling economic effects. Certainly, the supply logistics consequences of a terrorist attack on the ports—such as the extent to which port activities could be switched to still operational parts of the complex; the effects on domestic rail and truck operations; the consequences for importers in terms of lost sales, increased inventory costs, and use of storage space capacity and for trading partner economies; and the scope for trade diversion—are not fully accounted for, except to the extent that they are picked up in indirect effects in the input-output model. These supply chain implications would probably mandate behavioral adjustments that would mitigate the effects of an attack, either by post-event responses or ex ante preparations. Thus, their inclusion would not impair the overall argument that we are presenting upper-bound estimates.

Giving attention to one of these issues, to what extent could the remaining port facilities in the Los Angeles–Long Beach complex compensate for the loss of Terminal Island? Although it must be possible to increase throughput to some degree, our assessment is that the scope would be limited. The major constraint is the limited number of shipping berths. In recent years, trade has been expanding much faster than port capacity; this explains the relentless drive for port expansion. Another problem is the extent to which the unions would resist a move to 24-hour, seven-day-a-week operation. We believe that a successful terrorist attack on the scale envisaged would overcome the traditional resistance of the International Longshore and Warehouse Union (ILWU) to this change, but this is not assured. Yet another option is for the president to declare a state of emergency and order the National Guard or other military resources into the ports to accelerate freight flow through the remaining terminals.

The scale of potential economic damages suggests that there would be high societal returns from prevention and protection strategies. We have no knowledge of what is currently in place or what technological or personnel opportunities for prevention and protection now exist. Yet, given the span of these bridges, it is difficult to conceive that it would be possible to prevent an 18-wheeler loaded with conventional bombs from driving to the middle of a bridge, parking, and immediately detonating.

The more interesting logistical question is whether three such trucks could be exploded simultaneously (plus whatever is needed to take the rail bridge out) without intervening mishaps in terms of timing. If some access remained after the attack, the loss estimates produced in this chapter would be too high.

A further question is whether the bridges would be totally destroyed. It is impossible to predict this in advance. Damage to a segment of the span that kept the rest of the bridge in place would obviously be faster and cheaper to restore. Consultation on this issue with bridge engineers and bomb experts would be needed to attempt to answer this question. Given our argument that speed of restoration is the key to minimizing economic losses, this is a critical question.

An economic analysis of hypothetical terrorist attacks is difficult. Our approach is to consider vulnerabilities that might be seen as attractive to potential attackers. Terminal Island's large share of U.S. foreign trade and its few connections to the mainland are examples.

This approach is distinct from an approach based on the history of port closure effects caused by organized shutdowns by labor unions. These are always anticipated, giving all the parties time to make substitute arrangements and, thereby, dampen any adverse economic effects. As a result, we believe that past labor strikes have but limited value in predicting the outcomes from a terrorist attack.

Second, labor-related port closures may be inappropriate for comparison to a radiological attack. If the attack were radiological rather than conventional, the length of the closure would be a political decision and therefore of unknown duration. At some stage, the government could decide to bring in the military with protective clothing, but when that might happen is unknown and problematic.

Third, in the Terminal Island case, 55 percent of the output would be down for a significant period without the construction of temporary bridges. Such bridges would result in some access, but we have little idea about the consequential effects. Our results, always conservative, assume that the shipping lane problem from the temporary bridges would not interfere with subsequent trade.

Finally, it could be argued that the effects of a terrorist strike on Terminal Island would simply delay economic activity rather than

eliminate it. We believe that production and consumption delayed is not the equivalent of production and consumption denied. But even delays of production and consumption can result in significant transactions costs.

Conclusions

This chapter has demonstrated that a relatively simple terrorist attack (simultaneously blowing up three bridges plus a related rail bridge accessing Terminal Island at the Los Angeles–Long Beach port complex) could inflict massive damage to both the Southern California and the national economy. The extent of such damage depends on the length of the interruption in shipping activity, which in turn would depend on policy decisions regarding the pace of rebuilding: quick fixes such as temporary bridges or permanent bridge reconstruction. A benchmark annual estimate is $45 billion of output losses and 280,000 person-years of employment. These estimates can be scaled up or down according to the best "guesstimate" of the length of interruption. Also, our estimates are upper-bounded, and we have mentioned several mitigating interventions that might lower these losses. Regardless of the extent of these interventions, one clear implication is the high payoff of protection and prevention strategies (for example, what would be the full economic costs of inspecting every vehicle accessing the bridges?). Our research also suggests a substantial benefit, in the event of a successful attack, of ex ante prepared strategies to accelerate restoration.

References

Brunet, Alexia, "Protecting Our Homeland: Incorporating Terrorism Risk in State Homeland Security Grants," presented at University of Southern California, Los Angeles, California, December 15, 2004.

Cho, Sungbin, Peter Gordon, James E. Moore, II, Harry W. Richardson, Masanobu Shinozuka, and Stephanie Chang, "Integrating Transportation Network and Regional Economic Models to Estimate the Costs of a Large Urban Earthquake," *Journal of Regional Science* Vol. 41, No. 1, 2001, pp. 39–65.

Gordon, Peter, James E. Moore, II, Harry W. Richardson, and Qisheng Pan, "The Economic Impact of a Terrorist Attack on the Twin Ports of Los Angeles–Long Beach," in Harry W. Richardson, Peter Gordon, and James E. Moore, II, eds., *The Economic Impacts of Terrorist Attacks*, Edward Elgar, Northampton, Massachusetts, 2005a, pp. 262–286.

Gordon, Peter, James E. Moore, II, Harry W. Richardson, and Qisheng Pan, "Terrorist Attacks on Nationally Important Theme Parks," in Harry W. Richardson, Peter Gordon, and James E. Moore, II, eds., *The Economic Costs and Consequences of Terrorist Attacks*, Edward Elgar, Northampton, Massachusetts, 2005b.

4. Boom Boxes: Containers and Terrorism

Stephen S. Cohen
Berkeley Roundtable on the International Economy (BRIE)
University of California, Berkeley

> A single bomb of this type, carried by boat or exploded in a port, might well destroy the whole port with some of the surrounding territory.
>
> *Albert Einstein, in his famous letter to President Franklin Roosevelt, August 1939.*

> It is inevitable that terrorists will obtain weapons of mass destruction, and that they will use them against us.
>
> *Donald Rumsfeld, U.S. Secretary of Defense*[1]

Introduction

About 10 million containers arrive in U.S. ports from foreign countries each year.[2] (A comparable number go out, although about half

[1]Arquilla (2005), p. 6.

[2]As reported by Bowman (2005). The U.S. Government Accountability Office (GAO) uses the 2002 number of seven million in a December 2003 statement on developments in Maritime Security (U.S. Government Accountability Office, 2003). Robert Bonner, Commissioner of Customs and Border Protection, said 9.2 million on May 26, 2005, in testimony to the U.S. Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations. Nine days earlier, Robert Jacksta, Executive Director, Border Security and Facilitation, U.S. Customs and Border Protection, said 9.6 million to the Senate Commerce Committee. That same day, to the same committee, Christopher Koch, president and chief executive officer (CEO) of the World Shipping Council, said 10 million. The Pacific Maritime Association in its 2004 Annual Report states that five million containers arrived in West Coast ports, indicating that the national number should be at least 10 million and probably more. If you take the seven million number for 2002 and add the roughly 15 percent per year increase in trade, you get to 10 million by early 2006. The simple metric, how many boxes come in, as with so much in port security, seems to be surrounded by confusion.

the outgoing ones are empty).[3] They come from everywhere, carry everything, and go everywhere in America. A big container ship offloads about 3,000 containers in hours.[4] Typically forty feet long and weighing about 30,000 pounds, containers carry everything: axles, toys, sneakers, tiles, sinks, unpronounceable chemicals, faucets, clothing, food, tools, solvents, sunglasses, light bulbs. Occasionally, but we don't know how often, or in which containers, they carry things they shouldn't, such as bogus and unreliable auto and airplane parts, or people, or narcotics. Containers do not stay in port very long. They go out on trains and trucks and circulate almost everywhere, over bridges and through tunnels, to shopping centers, stadiums, and downtowns. Container security is not primarily about port security; it is about everyplace security. Indispensable and ubiquitous, a container is an excellent vector, or carrier, for weapons of mass destruction (WMDs) such as nukes or "dirty bombs."[5] Containerization is a technological innovation that, unlike semiconductors or genetic engineering, is intuitively easy to understand. Its effects have been huge. It has revolutionized international trade, made possible globalization, and, unfortunately, it is now necessitating a small revolution in U.S. defense. Why invest in intercontinental missiles when a container can do the job, with fine accuracy and at very low cost? A fully loaded container can be sent to the United States to arrive at its assigned destination, for example Chicago, on a reliable schedule, for well under $5,000. Containers change the rules and rosters: They are the poor man's missiles; you no longer have to be a big powerful government to create catastrophe.

This chapter discusses the threats that terrorists, using containers, pose to America, and measures to defend—deter and detect. It does not directly address reactions to attacks—what to do and what not to do in the event of an attack. Planning for such eventualities is vitally important. Along with inflicting direct damage, triggering self-inflicted damage, through ill-prepared reactions in an environment of panic, is

---

[3]Flynn (2004).

[4]World Shipping Council (n.d.).

[5]U.S. Commissioner of Customs and Border Protection Robert Bonner called containers "the potential Trojan horse of the 21st century" (Lipton, 2005b).

precisely the aim of terrorism. Nor does the chapter address the more fundamental question about overall defense strategy in an age of rabid terrorists with possible access to WMDs.

There are serious constraints on what can be done to deter or detect a container-borne attack on the United States. It is simply impossible to open and inspect each container that arrives without shutting down the international trade system and causing catastrophic economic damage. Unpacking a container is like unpacking a moving van; unpacking and repacking would take several people several hours.[6] Every day, about 27,000 containers arrive in U.S. ports from foreign countries, carrying well over 90 percent of imported cargo by bulk.[7] Containers carry almost $500 billion into the United States, of which about $165 billion enters through California ports.[8] They arrive and move through U.S. ports on tight schedules: companies such as Ford, Wal-Mart, and, most famously, Toyota, practice just-in-time inventory, which means that after a short while, if the containers do not arrive, everything stops; inventories are small. Tight, efficient supply-chain management has been singled out by no less an authority than Alan Greenspan as contributing significantly to the improved productivity of the U.S. economy and to our ability to hold down inflation and increase incomes.[9] It is relatively easy to find drugs that will kill off most diseases; the difficulty lies in finding measures to kill off the disease agents without killing or maiming the patient.

The first part of this chapter discusses container-borne threats and the constraints on measures to detect weapons concealed in a container. The second part traces possible itineraries for individual containers; it provides a concrete sense of the problem. The last part discusses measures to deter and detect.

---

[6]Flynn (2004), p. 87.

[7]Bowman (2005).

[8]Wein et al. (2004); Haveman and Hummels (2004).

[9]Greenspan (2001).

Threats

Terrorism, most analysts agree, poses two distinct kinds of threat. The first is severe direct damage: catastrophe. The second is terror, or the triggering of a destructive autoimmune reaction: an attack that precipitates reactions on our part that are themselves hugely more damaging than the initial terrorist act. Although useful for clarifying thinking, the distinction leads to problems in planning defense mostly because, as we shall see, there is a one-way spillover between the two categories: Massive direct damage provokes massive terror and self-destructive responses. Let us, nonetheless, begin by taking these two kinds of threat separately, starting with direct damage of catastrophic proportion.

Direct Catastrophic Damage

Perhaps any attack into America is An Attack on America, but not all attacks are the same. In surveying risk and defense, it is important to sort out threats, at least by scale of damage and plausibility, if not by statistical probability of occurrence. Damage is one thing; catastrophic damage is quite another; and although a scale consisting of regular gradations necessarily runs through them, the situation is really closer to the awful facts of combat triage, or clearing out an overstuffed attic, brutal sorting by crude category. "It is a truth universally acknowledged"[10] that we would be wise to concentrate our attention, resources, and efforts on preventing catastrophic direct damage and on averting massively self-destructive reactions to significantly more limited damage. But it is very difficult for a nation with a political system like that of the United States to do that in a hard-edged way and, therefore, imprudent to count on it. Although they can carry anything to almost anywhere, containers are especially excellent vectors for only two kinds of catastrophic direct damage. The first and worst is a nuclear bomb in a major city. New York or Washington, D.C., are the classic examples, but any city will do. Possibly hundreds of thousands of people could be killed instantly and many more times that number exposed to the risks of

[10]Austen (1813), p. 1.

slower death and suffering from burns and radiation sickness; economic and political dislocations will ensue that are, for practical purposes, of incalculable dimensions.

Dirty Bombs

A dirty bomb is the second threat of potentially catastrophic direct damage for which containers are choice vectors. But a dirty bomb blurs the clean line we just drew between a threat of disastrous direct damage and one that aims at triggering a disastrous autoimmune reaction; artfully placed, it can do both. A dirty bomb (also called a radiological dispersal device or RDD) consists of conventional explosives wrapped in radioactive material that on explosion shatters into particles that, depending on the bomb materials and conditions at the explosion site, can be more or less fine, and cover an area, of variable size, with radioactive dust of differing toxicities.[11] A dirty bomb is, in a way, the opposite of the neutron bomb of Cold War fame that purportedly killed people but not property;[12] dirty bombs essentially kill or paralyze real property while not, initially, directly harming many people. It is exceedingly difficult to obtain robust consensus of expert judgment about the direct damage a dirty bomb can cause. Fortunately, there has been no experience to inform estimates, and any estimate necessarily comes with a very full set of "it depends." It depends, first, on where the bomb explodes: on a ship in port? In a reasonably enclosed, or blocked-off area? Upwind or downwind from the sea? In Washington, directly in front of the FBI building? In the center of Manhattan at Times Square? It also depends, of course, on the scale of the explosion and the kind and the amount of radioactive material. It depends too on weather conditions (rain, wind) and upon the porosity of the materials that get dusted with radioactive matter: Concrete or dirt absorbs much more than polished granite or glass.[13] Most commentators agree that the number of people directly killed or immediately injured is likely to be

---

[11]American Nuclear Society (2002); Allison (2004), p. 57; Federal Emergency Management Agency (2002); National Defense University (2005).

[12]Scoville (1981).

[13]Nuclear Research Center (2004).

small, although again, that depends hugely on the kind of radioactive material used, distance, circumstances of diffusion, etc. In the hypothetical case of an explosion in midtown Manhattan, estimates range from several city blocks closed down for extensive decontamination, an effort measured in weeks, to the closure of the entire borough of Manhattan for very many years. All are good estimates; it just depends.[14]

It is possible to create estimates for the costs of almost anything, even the costs of Manhattan being, effectively, rendered uninhabitable; some people try to do the calculations.[15] The calculations themselves are pedestrian; the assumptions on which they are built are necessarily heroic. But like everything in this mass terror scenario, secondary effects overwhelm primary damages. Here they range, in economic terms, from changes in the value of the dollar and crashes in financial markets, to permanent shifts in the location of business activity, to questions of failures of the insurance system, and, of course, to the huge effect of reactions by governments, individuals, and markets. These conspire to make the World Trade Center event look, by comparison, unimportantly small. So much here is unknown and fundamentally unknowable. So much is mysterious and emotional: Radioactivity attack! Analyses of risk perception consistently report that the word "nuclear" generates much more fear than other risks of comparable magnitude,[16] although fear of the idea of an attack involving biological agents is growing. And containers can serve very satisfactorily as the terrorist's nuclear missile.

For most other weapons of truly mass destruction, containers are probably less the vector of choice: There are, regrettably, readily available, more suitable, alternatives.

---

[14]American Nuclear Society (2002); Allison (2004), pp. 56-60.

[15]Powell (2003) provides a sample: half a million dead, $1 trillion in economic damage. Paul Krugman (2004), p. 4, doodles with such calculations for a far, far smaller event.

[16]Herron and Jenkins-Smith (1996); Slovic (2000).

Biological and Chemical Weapons

Bioweapons, along with nuclear weapons, are arguably the most dreadful to contemplate in an all-star cast of horror scenarios. Airborne contagious diseases such as smallpox (regular or enhanced) could kill many millions of Americans (as well as spread around the world) quite quickly. But rather than import the disease in a container, terrorists equipped with smallpox would likely find it easier to infect a few willing (or unwitting) suicide attackers and fly them from Frankfurt or Dubai to Washington, New York, Houston, etc., with a change in London or Paris. Before any symptoms were manifest, before anyone knew what was happening, the hundreds of airline passengers who are now carriers would spread throughout the country and the world and in turn create devastating epidemics.[17] A ghastly inventory of attacks by infectious diseases could be extended to other infectious agents, but the key point here is that although seaborne containers do carry everything everywhere, they are better suited as vectors for some forms of devastating terrorist attacks than for others, especially nuclear weapons and dirty bombs.

Chemical weapons are a more complex and differentiated story and blend into the category of triggers for destructive autoimmune reactions. The most horrifying chemical weapons—nerve agents such as sarin and a bunch of dreadful others—are most effectively released in crowded, confined spaces: subways, air and rail terminals, megachurches, theaters and sports arenas, where they could kill hundreds, conceivably thousands of people. But they can be transported across borders, if indeed they need to be imported, in a simple glass bottle or two—the ubiquitous water bottle—carried in a suitcase, handbag, backpack, or even pocket. A container would be a serviceable import vector but a poor instrument for the lethal release of such a gas. The container would most likely serve only to transport the canister across our borders to a trusted terrorist agent, perhaps as a part of a case of wine, fruit juice, or salad oil, shipped along with a thousand other cases, and be efficiently delivered to a store or warehouse from which terrorist agents would get it and put it to use.

---

[17]On bioweapons and terrorism, see Stern (1999); Knobler, Mahmoud, and Pray (2002); "Biological Terrorism" (2005); Lawler (2001); U.S. Senate Committee on Governmental Affairs (1989); Bowman (2001).

But containers, unfortunately, are well suited for prominent roles in other kinds of attacks that employ chemical weapons. Those attacks, in addition to killing Americans, aim at creating terror and triggering reactions that themselves cause severe economic damage. Sometimes the number killed, by the most ordinary of chemicals, can be quite large. A container loaded with fertilizer (ammonium nitrate) could create a blast 10 times that of the Oklahoma City bombing.[18] As a result, priority for deterring and detecting chemical weapons must, in any realistic scheme of things, be increased to levels of effort far in excess of those based on the direct damage such weapons are likely to cause, because sociopolitical factors must be considered. A collection of chemicals that, when mixed, can cause explosions and release poisonous gas could be packed in separate canisters in a container—and the same thing done in several such containers, all scheduled to arrive in different inland locations within several days or even weeks. Manifests, which detail the containers' contents, could be falsified; this is not such an infrequent occurrence. There are many known cases, and an unknowable, but surely hugely larger number of unknown cases. The Organisation for Economic Cooperation and Development (OECD) tracked down two exemplary incidents:

In November 2002, a container exploded onboard the container ship *Hanjin Pennsylvania,* causing extensive damage. The cause was found to be improperly packed, improperly loaded, and improperly documented fireworks and calcium hypochlorite (a bleaching agent used in swimming pools) in containers. Again,

> Storm damage to the Santa Clara I off the eastern coast of the United States in January 2002 caused several containers containing magnesium phosphide to spill their contents in the hold. This compound, when mixed with air and/or water forms two highly reactive gases—phosphene and diphosphane—that can explosively auto-ignite at ambient temperatures. . . . In the case of the Santa Clara I, the magnesium phosphide containers were improperly manifested thus hiding the dangerous nature of their contents. This case of mislabeled containers is not a unique occurrence and, because of the constraints placed on hazardous compound handling and stowage both in ports and on ships, some unscrupulous shippers and forwarders ambiguously and/or mislabel containers containing these compounds. Anecdotal evidence from the port of Rotterdam

[18]Lipton (2005b).

> provides an indication of the extent of the phenomenon as recent container inspections have revealed that a significant number of containers containing Class 1.1 fireworks . . . were mislabeled as a less dangerous Class 1.3 and 1.4 fireworks—presumably to avoid the constraints, permitting costs, and delays imposed on the import of Class 1.1 substances.[19]

Disabling Autoimmune Reactions

Such cases are best likened to triggers of severe autoimmune reactions. A simple, scenario-planning example begins with a bomb, or chemical explosion in a container that came through a U.S. port. Then another one goes off, elsewhere in the country a day or two later, then another, five days later, and then a fourth. These events trigger the closure of all U.S. ports and a hugely costly interruption of trade. The direct damage from the explosions is rather modest; the economic damage resulting from the shutdown of shipping, depending upon how long it lasts, could be enormous as factories run out of spare parts, close down, and put a hold on deliveries from other suppliers; as stores deplete their stocks and lay off workers, etc.[20] A shutdown of one or two days would not be very costly and could easily be made up. Six weeks is a very different story. The problem fiendishly compounds if there is not one event but a series of three or four such container explosions in various points around the United States, over, say, a one-month or six-week period.

Simulation exercises are run to attempt to gauge the extent of economic damage and, more important, to pinpoint the reactions that cause the economic damage. They often begin by noting that al-Qaeda's communiqués released after the September 11 attacks stressed that one of its primary goals was to inflict massive economic losses on the United States.

One such exercise was conducted in October 2002, organized by the prestigious Conference Board. It estimated that about $60 billion in damages would result from a series of explosions (including, in a refined

---

[19]Crist (2003).

[20]Willis and Ortiz (2004), p. 10; U.S. Government Accountability Office (2004), p. 6; Harrald, Stephens, and van Dorp (2004), p. 3; Flynn (2004), p. 34.

touch, the discovery of containers with unexploded bombs inside) if ports were closed for eight days.[21]

This exercise mentioned, but did not tabulate, economic losses from stock and currency market panics, corporate earnings warnings, indirect business interruptions hitting airlines, hotels, shopping centers, and casinos, etc. Again, the purpose of the exercise was not so much to accurately estimate losses as to indicate how the U.S. reaction might cause the greatest avoidable losses and to prod thinking about how to avoid those same reactions in planning for a real event.[22]

It would be wise to prioritize our attention, resources, and efforts on catastrophic threats, which in the realm of containers means nukes and dirty bombs, and have rigorous plans in place to avoid severely self-destructive reactions. However, the basic forces of American politics and the dynamics of American society make any hard-edged decisions quite unlikely, whatever experts' plans may say. The likely scale of self-inflicted losses resulting from American reactions to a series of sub-catastrophic events changes the calculation of priorities and makes it necessary to extend efforts to defend against such threats to include those involving far less directly damaging explosives and chemical explosions. This, as will be seen, makes defense much more complicated, uncertain, and expensive.

Itineraries, Scenarios, and Documentation: Or, One Container, Two Containers, Three Containers, Four

Misdeeds concealed in shipping containers, such as stashing narcotics, or desperate immigrants, or counterfeit or smuggled goods, covered by bogus declarations of contents, are daily occurrences but not our concern in this chapter—except as an indicator of just how porous the system is. We will focus on weapons of mass destruction, and the easiest place to insert a WMD into a U.S.-bound container is, of course, when the container is being loaded in the first place; certainly not when

---

[21]Willis and Ortiz (2004), p. 17; Crist (2003), pp. 21–22.

[22]Harrald, Stephens, and van Dorp (2004), p. 2; Crist (2003), pp. 19–23, summarizes a similar exercise run by Booz-Allen.

it is aboard a ship. Lots of heavy stuff in irregular shapes such as engines and axles can be loaded into a container to make a nice, detection-reducing, central niche for the dreadful weapon. The container of choice should not, of course, originate in Afghanistan or Iraq or one of the "stans," or Indonesia or Pakistan or even Russia, the Ukraine, Egypt, or Cyprus. And it should not be addressed to a small apartment in Brooklyn. It should originate in a nice place, proudly carry the imprimatur of a respectable company, and embark as part of a routine shipping schedule. Documentation, of course, should be impeccable and routine. It should travel via giant, well-known ocean carriers. Every terrorist knows this as well as he knows his own very many names and that he should never, ever, purchase a one-way air ticket with cash. A hunt for anomalous shipping documentation, whether pursued by hunch or algorithm, will not catch the best of the attackers but is, of course, absolutely necessary: Sometimes the B-team strikes deadly blows.

To get a sense of the concrete reality of the problem, let us follow the itineraries of typical in-bound containers, starting with the simplest and adding complexity; and we must recall that some ten million of the boxes arrive in the United States every year, on tight schedules.

Simple and Less-Simple Itineraries

The simplest scenario involves a container that is fully loaded at the plant of a trusted company and shipped, in regular sequence, say as an instance of a routine, once-a-week shipment to the same destination. Assume that Mercedes loads it at a plant in Eastern Germany, or France, or Belgium. The contents, heavy auto parts, mostly, although not entirely, steel (there is also a lot of aluminum, copper, plastic, rubber, electrical circuits, and even some chemicals as well) are loaded at the shipping gate, the container closed and sealed, the box transferred by rail to the port of Antwerp. But packed and locked by whom? If a major concern is penetration of the supply chain by Islamic ultra-radicals, the workforce in each of these European allies, outside the executive offices, at the points of actual loading, moving, transferring, waiting, and watching, is heavily Islamic and penetration of these communities by radical fundamentalism is now epidemic.

Another WMD container scenario could plausibly begin at a plant, say, 400 kilometers inland from Shenzhen, where low value-added manufacturing is rapidly relocating from the relatively high-cost cities of the Pearl River Delta.[23] The load consists of small electrical appliances, coffee makers, alarm clocks, toasters, small refrigerators, and clothes irons. The company, Wong Products, can be found in the databases of U.S. authorities: They ship frequently, at least six containers per year, although not at regular weekly or monthly intervals. The destinations differ: Their products do not all go to Wal-Mart. This one is destined for a volume retailer in Chicago, known to U.S. authorities, and is to travel via Guangdong, Hong Kong, and the port of Los Angeles. The ocean carrier is well known to U.S. authorities, one of a handful of international giants that dominate the business, and "trusted."[24] The guys loading the container at the plant are paid about $3 to $4 per day, the driver too. They load the container, lock it, and seal it. Someone else signs off on the bill of lading that describes the contents (although he is in another building and only comes by late in the afternoon, when the pickup is scheduled whether it is happening or not). The paperwork is then sent electronically to the railway that will forward it to the river barge company, which will, in turn, pass it on to the ocean carrier who will send it to U.S. customs.[25] The driver takes the load and begins his trip to a railroad yard, where he is to drop it, for handoff to a river barge company, and to then pick up an empty. If all goes well, in terms of road traffic and delays as well as other frequent problems, he has a six-hour drive. But today there were delays (engine problems on the rig en route to pickup), and he gets a late start, too late to arrive at the drop-off station before it closes at 6 p.m. This often happens, despite repeated efforts to improve the truck's maintenance, and he tends to spend the night at a girl friend's house, a house where there are many such girl friends, and many such trucks. In this case, there are two fine opportunities for inserting a WMD: The best is at the initial point of loading. The second is where the container spends the night.

---

[23]"China's Manufacturers Sing Pearl River Delta Blues" (2004).

[24]Harrald, Stephens, and van Dorp (2004), p. 3.

[25]Frittelli (2003), p. 12.

Tampering is not that difficult; the lock is cheap, the seal even cheaper, the hinges easily removed and replaced. Nor, after some practice, is simply switching containers all that difficult with, of course, the correct ID numbers and duplicate locks and seals affixed to the substitute container. This is a simple scenario, with one cute wrinkle. It can be made more complicated, and the container more and more vulnerable.

Mixed Loads and Complicated Itineraries

Mixed loads are more challenging. Some 40 percent of all containers arriving in the United States are mixed loads, that is, they contain cargo consisting of quite different things from several points of origin, stuffed together in one box.[26] The container can be filled at a shipper's warehouse, to which all the products have been delivered, or it can be filled, one stop at a time, at different plants. Let us follow the latter, less frequent, itinerary and stylize it.

The container is first loaded at Lee products, the same general location as the previous example, with 10,000 pounds of floor tiles, in 44-pound cartons. It is then closed, but not locked or sealed, and hauled 10 miles over bad roads to another factory, Lu Industries, where it spends the night, locked. ("If you can break into a locked gym locker you can break into the container.")[27] The next day, a second load consisting of 15,000 pounds of auto parts (of bogus BMW branding), in crates of varying size, is stuffed in. The box is locked and sealed by the alcoholic nephew of the assistant plant manager who is the son of a local deputy crime boss. At a third point of loading, 17,000 pounds of machinery (on pallets) come aboard and the box is locked and sealed.[28] The container is then driven to a railroad yard, where it spends 72 hours, 24 of them in the dark, with lots of company: thousands of other boxes and two guards, equipped with flashlights, somewhere out there in a poorly heated shack. They are paid about $3 per day. (As the cliché of this business goes: A box that is not moving is a box at risk, and the

---

[26]Flynn (2004), pp. 89-90.

[27]Van de Voort et al. (2003), p. 9.

[28]The metal, steel, and aluminum in the machinery and the irregular distribution of the machines in the container make detection all the more difficult (Wein et al., 2004).

average container makes 17 shifts.[29] Ocean shipping of containers is not mostly about boxes on ships; it is "intermodal" in the extreme. There are lots of opportunities for serious mischief.) The container is then hauled to the port, where it is transferred to a big oceangoing ship, along with about 3,000 other containers. The documentation is provided to the ocean carrier by the shipping company that employs the trucker and assembled on the basis of what each plant reported to it, and the ocean carrier forwards the documentation on to U.S. Customs.[30] The importation of counterfeit goods is not a problem of direct concern in this chapter. But it is of interest as an indicator of the unreliability of information provided to U.S. Customs about the contents of containers and the pressures under which the agency must operate. The volume of such fraud seems to be enormous: The huge amount of counterfeit goods, ranging from auto and aircraft parts through pharmaceuticals, handbags, watches, and sneakers that enter this and every other country testifies in unimpeachable quantity to the untrustworthiness of shipping documents and the ease with which untoward cargo can be shipped in containers. *Business Week* boldly brandishes an estimate that counterfeits represent some 5 percent to 7 percent of world trade.[31] If it is even in the right ballpark, that is a colossal quantity, and few of those "genuine" designer handbags sold on the street in almost every city in the world, or the auto parts that fail at crucial moments, or even counterfeit aircraft parts come by air: Most come by sea, in containers. They are indicators of porosity and so, of course, are narcotics shipments, the object, presumably, of massive, systematic, and exceedingly expensive vigilance. They point to big weaknesses in the system.

"Container Bob" and Other Indicators

We have every reason to suspect that the documentation that declares just what is in a container, and where it comes from, is often incomplete, misleading, or outright falsified: certainly not in a near majority of cases, but often enough to indicate a very serious problem.

---

[29]Flynn (2004), p. 89.

[30]Flynn (2004), p. 106.

[31]Balfour (2005).

The best and most readily available indicators are of course those rare cases when a container is opened and something quite unexpected (as well as undocumented) is found. Most famously, and probably most embarrassingly, two years after the September 11 attacks, an ABC television news crew demonstrated the potential for inconsistency between documents and contents, as well as the porosity of the system to the most dreaded cargo, when it successfully smuggled a container packed with 15 pounds of depleted uranium from Jakarta to the Port of Los Angeles by simply not declaring the box's contents.[32] After the ruse was broadcast, apologies were profusely rendered, mostly by ABC. There are numerous examples of things being found in containers that should not have been there. In mid-January 2005, some 30 or so Chinese streamed out of two separate containers in the Port of Los Angeles. What security system spotted them and alerted the port authorities? The unionized crane operator saw three men climbing out of a container and phoned the police.[33] In much of the discussion about port security, dockworkers are seen as a potential source of problems for which new policing techniques are needed (for example, much of the talk surrounding the proposed introduction of a Transportation Worker Identification Credential, or TWIC card). Of course, terrorists working as dockworkers and, even more dangerously, drivers who haul the containers out of the port are a real danger: They are the perfect vector to take the offloaded container that carries the WMD and deliver not to Target as the documentation states, but to its target. Drivers hauling loads out of ports are not the kind of regular workforce that the dockworkers constitute. Drivers earn wretchedly little and have a turnover rate of 30 percent per year, making it difficult to screen that critical segment of the workforce.[34] But the workforce at home and abroad would best be understood and used as first-line responders as, to mangle metaphors, the hands-on eyes of the port and supply chain. There have been many cases of containers supposedly packed with

---

[32]Kates (2003); Kurtz (2003). For a less colorful account, see Skinner (2005).

[33]Associated Press (2005).

[34]Wein et al. (2004).

equipment and parts carrying along an undeclared Mercedes into, let us say, Malaysia, as a payoff to Malaysian customs or other officials.

And then there was "Container Bob," a legend in port security circles. Five weeks after the September 11 attacks, in the giant Italian container port of Gioia Tauro, which handles about two and a half million containers a year, authorities, alerted again by a dockworker, discovered a stowaway within a container that was carefully and tastefully appointed for a long voyage. It had a bed, a heater, and a toilet. The man also had a satellite phone, a cell phone, a laptop computer and, most curiously, airport security passes and an airline mechanic's certificate valid for Chicago's O'Hare and New York's Kennedy airports. Curiouser and curiouser, after his arraignment, he was released on bail and disappeared. The container in which he had booked such first-class passage was chartered by Maersk Sealand's Egyptian office and loaded in Port Said onto a German-owned charter ship, proudly flying an Antigua flag. It was to stop again in Rotterdam and then go to Canada and from there overland to Chicago (I have been unable to find out what the documentation that accompanied that container declared as its contents, or its initial point of loading). The stowaway was trying to punch a small hole into the side of the container, reportedly for better ventilation, or perhaps to have a view of scenic southern Italy, when the dockworkers spotted something amiss; otherwise he would have continued his journey, right on schedule, and perhaps into history.[35] "Container Bob" is an extreme case; then again, that is precisely what we must defend against, and his itinerary, outlandish as it might first appear, follows quite closely those of our scenarios above.

The scenario can be made much scarier without resorting to the automatically suspect examples of shipments originating in Pakistan, Afghanistan, or Iraq. Steve Flynn, a former Coast Guard commander and White House security staffer, does so, in hurried brushstrokes:

> Anyone who has $3,000 to $5,000 can lease one of the many millions of containers that circulate around the globe. They can pack it with up to 65,000 pounds of items, close the door, and lock it with a seal that costs a half-dollar. The box then enters the transportation system. . . . Accompanying documents

---

[35]Falk and Schwartz (2005); Crist (2003), p. 9.

> usually describe the content of the cargo container in general terms. If the box moves through intermediate ports before it enters the United States, the container manifest typically indicates only the details known to the final transportation carrier. For instance, a container could start in Central Asia, travel to an interior port in Europe, move by train to the Netherlands, cross the Atlantic by ship to Canada, and then move by rail to Chicago. The manifest submitted to U.S. customs inspectors often will only say that the container is being shipped from Halifax and originated in Rotterdam.[36]

Defense

How to defend? No one measure, procedure, or technology will provide a very high (90%-plus) probability of spotting a WMD carefully concealed in one of the 10 million containers arriving in the United States; 100 percent is pure fantasy. Furthermore, defense is a game not against nature but against smart and resourceful antagonists. New defensive measures will generate innovative attack countermeasures, and so on, as it has evolved throughout the history of combat, not to mention crime. A decisive, preemptive, military strike (as in "take them out before they can strike us") for this new war with multinational, loosely networked terrorists would be a temptingly cathartic but an inappropriate and unreliable strategy; an advance tip-off through intelligence, however, would be of enormous value but too uncertain to count on. The strategy that appears best is to create layers of security through which containers must pass, each layer different, in what it can do, how it does it, and what it depends on for success. Each one alone may be woefully unreliable, adding, say, a 33 percent chance of spotting a weapon, but if the container must pass through four such systems, the odds climb to 81 percent. A similar series of 50-percent-reliable "WMD spotting steps" pushes the chances of finding a weapon up to 94 percent. But the real world imposes severe constraints on this popular model of simple cumulative probability. The security system must operate in a context of rapid, high-volume movements and very minimal delays. So, for example, an inspection technology that is 50 percent likely to spot a weapon has an altogether different value if it includes a 20 percent probability of a "false positive." Almost any known inspection system

---

[36]Flynn (2004), pp. 88–89.

will yield false positives. But a false positive is not at all the same as a false negative or an omission. A false negative will go right on through, most likely without consequence, possibly with disastrous result. To be effective, the system must be able to review false positives quickly through non-intrusive means. In the post–September 11 flurry of well-meant efforts to "do something," various legislators have proposed new security measures; some even proposed legislation that would call for hand inspection of each container.[37] A container is roughly the size of a moving van, 40 feet long and fully packed; the labor time involved in unpacking, inspecting, and repacking it dockside would bring the entire system to a halt or at best to an economically ruinous crawl, inflicting, by ourselves on ourselves, the terrorists' ambition.

Layers

One group of researchers has enumerated 11 layers in a hypothetical security system;[38] others provide variously four to six such layers.[39] However they define and count their layers, most are quite similar in the kinds of measures they call for, although they may differ in important ways about what should be done in each. They call for new measures in (1) intelligence, (2) the early provision of more and better information and documentation about container contents, (3) activating shippers, all the way up and down the chain, to greater procedural uniformity, fastidiousness, and vigilance, (4) greater control and background screening of those having access to containers and ports, and (5) developing and installing new inspection and tracking technologies.

Improvements in security against terrorists employing containers must necessarily happen, to a greater degree than perhaps one would wish, abroad. This is not the same as the bold projection of force abroad—to head them off at the pass. Rather, it means that most security measures must be implemented by foreign nationals, companies, and governments on their turf, often at considerable cost and bother to themselves, and sometimes for reasons that they do not all support with

---

[37]Flynn (2004), p. 87.

[38]Wein et al. (2004), p. 1.

[39]Willis and Ortiz (2004), p. 7.

unquestioning enthusiasm. Much must depend on diplomacy, on the kindness of strangers, and, preferably, on their self-interest.

Intelligence

The first level of helpful activity from foreigners is intelligence, advance information—even on-the-spot police action—about a terrorist effort to attack. I am in absolutely no position to comment on the efficacy of U.S. intelligence in these matters. One can note that in the analogous, but vastly less important, history of narcotics interdiction, the record has not been reassuring. The vital need for just such intelligence and cooperation is obvious—it can be invaluable; it just can't be day-in and day-out reliable.

Early Provision of More Complete Information, Greater Procedural Uniformity, and Greater Access Control

Here there has been movement since the September 11 attacks. Ocean carriers are now required to send U.S. Customs and Border Protection the manifest for each container, electronically, in a standard, machine-readable format, 24 hours before loading at a foreign port.[40] This is an improvement. Customs is developing necessarily secret algorithms to analyze the data on the container to spot anomalies. It is assumed that these algorithms will improve as they process more and more data and gather experience. But even such technically elegant and sensible systems can be foiled: A group of American academics has shown how a well-organized and patient terrorist group could send a substantial number of containers through the system, each with some little difference in documentation, and analyze which ones get held up. So the game constantly ratchets upward.[41] At the core of all difficulties in dealing with incomplete, incorrect, or falsified manifests (lists of what is in the box and where it comes from) is one simple, recalcitrant fact. The shipper who forwards the information on to the next step in the chain gets that information from the previous step. Those at the initial point of loading declare what is in the box; all the rest of the information

---

[40]American Shipper (2002). See Crist (2003) for a tidy summary.

[41]Wein et al. (2004) explore gaming the system.

is secondhand, passing on that initial declaration.[42] It is rather like the way you send a package via Federal Express or UPS. You declare what is in the box, not FedEx.

Proposals to radically re-engineer, not just marginally strengthen, that very weak link in the security of the supply chain have been advanced. They boldly posit that all U.S.-bound containers must be packed only in certified loading facilities abroad operated by "trusted" agents.[43] A trusted agent could be a company known to U.S. authorities that makes very frequent shipments, such as Sony or BMW. Or it could be a special loading facility operated by a shipping company approved by U.S. authorities, such as Maersk or Hutchinson, two of the four giants in ocean container shipping. Further, the facilities would be inspected, certified, and monitored by U.S. government agents and equipped with a full panoply of security devices, ranging from tightly controlled access, with full background checks and tamper-proof ID cards for workers, through time signature digital photos of everything being loaded, and all kinds of inspection devices to peer through the cardboard, not steel, boxes that would be delivered to the facility for containerization. The fact that some 70 percent of all containers coming into the United States pass through facilities operated by just four giant international shipping companies makes this proposal a bit less of a stretch.[44] Such a reconfiguration of the conduct of international trade would go a long way toward reducing the danger of a WMD arriving in a container, but it is a very radical change. It is not surprising, therefore, that such proposals have met strenuous rejection up and down the supply chain and beyond. The bases of opposition are economic and political. Cost first. Such a change would dramatically increase the costs of shipping goods to the United States, probably by quite enough to figure prominently, and unhappily, in national cost-of-living and inflation data. And, unlike proposals to inspect all containers at U.S. ports, the Keynesian-scale spending of these proposals would all go to job creation

---

[42]Van de Voort et al. (2003), p. 5; World Shipping Council et al. (2004); Flynn (2004), p. 89.

[43]Flynn (2004), p. 93, lays out such a proposal.

[44]Flynn (2004), p. 93; Hasbrouck (2004).

abroad. It would also exert a palpable downward pressure on, for example, Chinese exports and, therefore, production and employment, something the Chinese government has gone to extraordinary lengths, as in foreign exchange markets, to avoid. It would also be a negative business factor for giant retailers such as Wal-Mart that rely on huge volumes at low prices and on the tightly stretched purchasing power of their income-constrained clientele. It would also cause a major reconfiguration and consolidation of the logistics industry in many foreign countries and in the United States too, once demands for security reciprocity were imposed. There are some 40,000 companies worldwide in the container freight consolidation business.[45] They employ about 8–10 million people.[46] Such a change would also pit city against city in cutthroat competition for the location of such facilities and the attendant employment. And for those who favor competitive markets and competition, it would create oligopolies with enormous market power. Such measures are not likely to be implemented, at least not before a container-carried attack.

Documentation should be improved, recognizing the fact that it is the box stuffer who declares what is in the box and nobody checks that initial step. The reforms, as mentioned above, call for sending the manifest information sooner (before the ship leaves the port of embarkation), in electronic format, with greater completeness, etc. For such reforms to work, they must be tied to a U.S.-government-imposed system of rules and regulations, rewards and penalties, to encourage not just conformance, but active, day-to-day, long-term vigilance—and all of this taking place outside the United States. And they must be obligatory, not voluntary.[47]

Technologies

As documentation cannot be taken as trustworthy, and as it is quite impossible to open each container, unpack it, and look inside,

---

[45]Crist (2003), p. 25.

[46]Crist (2003).

[47]The Government Accountability Office describes and evaluates these and related programs (Wrightson, 2005).

technology—to peer, poke, and sniff at the contents—becomes the imperative instrument of defense, even if it does not yet quite exist. Detection technologies can be put in two places: in-port or in-box. A third kind of technology is necessary for both: information systems to relay, organize, and sift through all the data coming in from advance notice manifests and from in-box sensors once installed and to analyze the data against huge databases of possibly pertinent information. This kind of homeland security database technology, data-mining, is becoming a serious "business opportunity," as well as the subject of controversy and privacy problems (which, for containers, are significantly less than, say, for airline passengers). Its ongoing development and deployment is taken as a given in this chapter.

Non-invasive inspection technologies, roughly speaking, either look into the box or sniff it, without opening it. Visualization or imaging technologies peer into the box using x-rays or gamma rays to construct an image of the contents; these images, like their medical counterparts, can be more sophisticated than a simple black and white photo. Sniffers seek out telltale traces of chemicals or isotopes. Visualization technologies are active in that they shoot something (x-rays) into the box. Sniffers, including critically, radiation detectors, can be either passive—just sensing emitted isotopes—or active—shooting something into the box to prod emissions, which are then detected.

In-Port Imaging. Non-intrusive imaging is analogous to medical imaging that peers through your skin without opening it, such as, classically, x-rays, to see what is inside. Using either x-rays or gamma-rays, these machines peer though the steel container to produce images of the contents. Those images are then examined to see if the contents square with what is supposed to be in the box.[48] Are there, perhaps, steel canisters where there should be cardboard boxes of shoes, toys, and auto wheels? The machines can snap an image quickly; a box can pass through some of them in about 30 seconds. But not just anyone can read the image. Think of a medical image. Interpreting it takes a trained eye, and it might take more than a few seconds or even minutes.

---

[48]Harris (2002).

(Do remember how important time is in port logistics.[49]) In some ports (several sections of the megaport of Rotterdam), it takes 20 minutes to drive from the terminal imaging site to the outer gates—time enough to study the image and stop the truck at the gate should something untoward appear. Elsewhere, configurations differ. One answer to this problem is, of course, more technology: powerful computers and software to scan the images and quickly compare them to vast inventories of suspicious prototypes. These too are in development—part of a bubbling mini-sector of homeland security technology developers and vendors. One market analysis firm lists about 150 companies in its very selective coverage roster, ranging from IBM through ambitious start-ups and agile retreads.[50] A less-elegant solution, but one entering common use, is to lay the containers out at portside and pass the scanner over them.

Obviously, it is prudent to take such scans at the port of embarkation where the box could still be pulled before sailing should something untoward appear on the screen, and from which the file can be transferred to stateside authorities for a less-hurried second opinion (also to serve as a check against the unlikely case of shipboard insertion of a WMD). That would also leave adequate time for further enquiries and, in the worst case, for the ship to be diverted. The preferred alternative is, therefore, a two-step process—imaging at both ends. A good deal of progress has been made in readying such technology. They are in use at U.S. and foreign ports and deployment is accelerating. Some simple, but awkward, problems of implementation have been overcome. One was the fear, prevalent among drivers who haul the boxes, of health effects from exposure to the machines' radiation: they do not want to pass through the "x-ray" machines several times a day. A solution is for the giant crane that lifts the container off the ship to place it directly onto a waiting chassis that moves automatically, with no driver, through the inspection machines and out to the terminal gate where it is transferred onto waiting trucks, trains, or barges. One terminal at the Port of Rotterdam now operates this way, but U.S. ports

---

[49]Wein et al. (2004), p. 21; interviews.

[50]Civitas, and also ABI Research.

are very, very far from such a degree of automation and technological sophistication. A workable solution has been developed in America's megaport, Los Angeles/Long Beach, which can only dream of achieving the technical sophistication and efficiency routinely achieved at Rotterdam and Hong Kong. The unloading cranes align the containers on the ground in long, parallel rows—like trains. The imaging machine, mounted on tall steel legs and wheels, then passes over them. The machine does several sets of rows at one terminal, and then lumbers over to the next one, thus cutting down on the number of machines needed to service the port. These machines are not cheap; some can cost up to $1 million, not including operating and maintenance costs. Their deployment is increasing but results are mixed. Too many false positives is the typical, informal, judgment.[51]

The U.S. government buys and operates these machines. And although it might make the best sense for it to do so in terms of both integrity and authority, and so as to be able to require foreign customs officials abroad to operate their own equipment, determining who should pay for this "required service" is quite another question. Customs agencies traditionally pay for their own examiners and equipment. But a user-pays system such as a fee per box would, first, take a cost item off one little line of the homeland security budget. The cost would then spread up and down the supply chain and not be levied on the taxpayer. It might also permit more rapid innovation, precisely by getting the cost out of the budgetary process; the toll bridges that many containers must cross are not all that different in terms of economic rationale.

The second kind of in-port non-invasive inspection technology is radiation detectors (in our terminology, "sniffers" as opposed to "peerers"): They detect traces of radioactivity. Detectors used today are passive detectors. These come in many varieties, including handheld devices, and are substantially cheaper to purchase and operate than the imaging machines. The well-known Geiger counter is an early example. Drive-through radiation detector portals are already working quite well,

---

[51]Interviews, rather than published, more scientifically based materials, are the main sources for this paragraph. Lipton (2005a) summarizes interviews by the *New York Times* more authoritatively. See also U.S. Government Accountability Office (2002).

in terms of logistics, at U.S. ports: They are quick, nearly imperceptible, and pose no health problems.[52] The low cost and easy portability of some models makes possible ubiquitous detection, although most containers do not make that many stops between being loaded on a ship and clearing the port on arrival. But passive detectors have limitations, and, in their line of work—radiation detection—all limitations are serious. Radiation is emitted not just by concealed nuclear weapons, but also by legitimate and ordinary shipments that include many kinds of common goods such as tiles and bananas. The machine, and its backup information technology system, must be able to distinguish the radiation emitted by tile, bananas, and, famously, kitty litter, from that of cesium or cobalt and the like. And, as shown above, it must do this with a very low proportion of false positives without abandoning the struggle against false negatives.

So far, false positives are proving to be frustratingly frequent.[53] Further, and substantially more disturbing, it is not at all certain that passive radiation detectors can detect a well-shielded dirty bomb. Wein et al. (2004) report on one kind of in-box passive radiation sensor, neutron detectors (there are also gamma detectors): ". . . even after seven days of testing in our model, the passive neutron sensor is unable to detect a plutonium weapon with the maximum amount of shielding, and no improvement over the base case is possible."[54]

And the more the detectors are tuned up to improve their sensitivity, the more false positives.[55] Interviews with highly knowledgeable nuclear detection experts reveal that plutonium is somewhat easier to detect than U-235. It emits more radiation per gram of material and plutonium

---

[52]Alex Veiga of the Associated Press reports that Homeland Security Secretary Michael Chertoff stated on June 3, 2005, that the giant port complex of Los Angeles and Long Beach would be fully equipped with such detectors by the end of 2005. Oakland already is, with a complement of 25 machines, at a cost of about $250,000 each. They take about five seconds to scan a container (Veiga, 2005).

[53]Customs and Border Protection Commissioner Bonner mentioned 10,000 of them in his testimony to the U.S. House of Representatives Appropriations Committee, Subcommittee on Homeland Security, March 15, 2005 (Bonner, 2005); see also Lipton (2005a); Lane (2004).

[54]Wein et al. (2004), p. 22.

[55]Lane (2004) treats this very well.

emits neutrons (which U-235 does not). A tech-savvy and well-informed terrorist could put in enough shielding to defeat any one—perhaps even several—detection modalities.

Active In-Port. Active systems can detect both U-235 and plutonium, but they do not quite yet exist in tested, deployable models. They are much more complicated devices and more expensive too. They operate not by catching and detecting emitted radiation; they emit their own radiation to prod radioactive sources to emit detectable signatures. These are in development at places ranging from giant national laboratories through very small start-ups. We are told that the federal government has funded a substantial (around $100 million) research program. Much about them is, understandably, held secret—although at the same time hyped. The simplest questions this technology presents concern timing: Should existing, but quite imperfect, technology be installed now? Or should we wait? The need, after all, is now, and we must have something. If we wait, when will new technology become available? How well will it work? How reliable will it be, not just in terms of time "up and running," but, crucially, in generating false positives (and false negatives)? How fast will active systems run and how much will they cost? What new problems will they present or create? Nothing authoritative is publicly available to use for addressing these questions. Perhaps that is as it should be. Our own estimate is for tested prototypes in about a year.

In-Box. "Sniffers"—in-box sensors—to detect radiation, people, light, motion, temperature, humidity, explosives, specific chemical traces, etc., constitute another distinctive layer of defense. They figure prominently in most proposals for getting serious about container security, as well as in the Department of Homeland Security's ambitions to significantly improve port security. U.S. Customs and Border Protection Commissioner Bonner announced that the department is eager to quickly adopt in-box sensors and radio frequency identification (RFID) technology for container tracking.[56]

The sensors, placed securely inside the container, should be able to operate all the time or, if that poses a difficulty (perhaps because of

---

[56]Frontline Solutions (2005).

limited battery power), switch on and off frequently, taking real time readings and relaying them via radio frequency or some alternate communications technology to U.S. authorities. Location tracking as well as detection is integral to almost every proposal. (Indeed, tamper-proof locks and location trackers invariably come first on every list; they are far cheaper than sensors, are already proven, and carry a positive commercial benefit. They show if the container has been opened and where it is; unfortunately, they do not detect weapons or improper cargo.) The sensors would operate from the time of loading all the way through the point of unloading.

Reliability is a critical concern: False positives would bring down the international trade system or else could make the sensors into something like car alarms in a city, angering and ignored. Commissioner Bonner, aware of this problem, sets the date for rapid adoption for "as soon as the technology to reduce false positives to an acceptable level is there to do so, and not a day later."[57] Cost is another consideration. There may be a very limited number of high-volume container ports in the United States, but there are about 15 million containers in circulation worldwide.[58] Even with a resulting selection of containers suitable for shipment into the United States, that would still leave several million to equip. The cost of active detector systems as discussed above for in-port use, barring a thousand-fold fall in their price, is simply out of the question: Millions of containers at a million dollars each yields federal budget size numbers. In-box means, therefore, passive. But because findings are transmitted to the next lines of defense, false positives need not result in the delays and costs associated with in-port false positives.

Cost estimates for equipping containers differ considerably. The cost for tamper-proof locks and location trackers is low.[59] The most common number that includes sensors, and not just locks and RFID, is $500.[60] This amount nicely generates estimates of commercial benefits

---

[57]Frontline Solutions (2005).

[58]Van de Voort et al. (2003), p. 12.

[59]Van de Voort et al. (2003), p. 6.

[60]Flynn (2004), p. 100.

such as the $1,200 per container by one vendor, Savi Technology.[61] But doubling that cost to $1,000 seems prudent while still remaining useful for our purposes. The initial total cost number seems a bit shocking: $15 billion dollars to equip the container fleet. But not all containers need be so equipped. Assume that only three million containers need to be equipped with sensor kits to make them admissible to the United States (10 million arrivals, a bit over three round trips per year per box). It is likely that an equal number of containers would have to be comparably equipped to service other countries that would, reciprocally, impose similar rules. However, the equipment should serve for five years, so that brings the cost down to $200 per container per year, or about $75 per round trip. The per trip cost falls if each equipped container, given the new incentives, is used for yet more round trips per year, an outcome for which the costs provide incentives.

In this case, radio frequency tracking and 24/7 remote sensor operations outlays, unlike outlays for the other security technologies, constitute only one part of the net cost equation; there are some very real commercial benefits to be expected. Estimates of such savings differ in amount, but they attribute most of the savings to location tracking, the reduction in number of temporarily lost boxes, and the strong positive effect of improving supply chain management. Here, too, the variations are so great as to indicate the need for further research. Michael Nacht estimates a $1 billion per year saving from container tracking.[62] A partnership of two consulting firms pops for $10 billion.[63] The OECD estimates $26 billion (mostly from use of electronic manifests) over a 20-year period.[64] Flynn cites a preliminary study by a group of shipping companies that found a savings of $400 per $70,000 of cargo from tracking and electronic documentation, which translates, crudely, to $2 billion per year for imports alone.[65] As long as nothing goes dreadfully wrong, the commercial benefit would be realized not from the sensors

---

[61]Frontline Solutions (2005).

[62]Nacht (2001), p. 4.

[63]Inbar and Wolfe (2004).

[64]Crist (2003), p. 4.

[65]Flynn (2004), p. 109.

inside the box but from a much-improved container seal ($25 is an often-quoted price for one that is "smart" and supposed to last 10 years without needing recharging) and from RFID location-tracking systems that are also relatively cheap.[66] As opposed to the sensors, these technologies are pretty much off-the-shelf. The sensors are not. Some are being sea-tested. Many companies, ranging from giants such as United Technologies and Level 3, to small Silicon Valley firms such as Rae Systems, are developing products for what a busy population of market consultants and analysts tout as a market set for explosive growth.[67] The locks, seals, and location technologies are clearly useful and well on their way to deployment. They do not, however, adequately deal with the core problem—the weapon of mass destruction concealed inside the box. Here the sensors are critical. But beyond the formidable problem of false positives, the difficult one of costs, and the unknown facts of their ability to detect well-shielded dirty bombs and U235, they pose another set of questions. The first is operating and maintaining the systems. Who will make sure that the sensor systems are in good operating order before the container is loaded? Unlike the relatively few, big, in-port-inspection machines, these millions of sensor-equipped containers, scattered all over the world, cannot be controlled, maintained, or operated by government authorities. There is also the non-trivial problem of tampering or foiling. Terrorists could easily arrange to have control of quite a few sensor-equipped containers for long, undisturbed study periods. So the sensors that survey container security must, themselves, at a minimum, be "tamper-proof" and securely encased and provided with their own sensors to detect tampering.

---

[66]Fortner (2002).

[67]See ABI Research (2005); Beckner and Shaheen (2005); Wolfe (2002); Inbar and Wolfe (2004). For United Technologies, see "Looking for a Big Market? Try Container Security" (2005). On sea testing for in-box detectors, see Rae Systems (2005).

Conclusion

There can be no concluding; it goes on and on and, if all goes well, will continue to. Ten million boxes come in; one of them could be Pandora's.

The Threats

The principal threats from seaborne containers are (1) a nuke or dirty bomb that would inflict catastrophic direct damage, and (2) a series of conventional explosions that trigger reactions by American authorities and citizens that inflict severe economic damage on the U.S. economy.

The Constraints

It is not possible to open each in-bound container, inspect it, and repack it without inflicting on ourselves just the kind of economic damage terrorists hope to cause. Inspection must be quick and overwhelmingly non-invasive (boxes stay closed).

The Approach to Defense

No single defensive measure can provide a high probability of detecting a weapon of mass destruction, let alone more conventional weapons, inside a sealed container. A "layered" system of defense, traditional in military history beginning with medieval fortifications is, therefore, the generally accepted model. However they are stacked, the layers come down to a small set of key, but not simple, defensive measures:

Intelligence

Intelligence can be invaluable, but it can never be day-in, day-out reliable, and there are no associated cost estimates.

Documentation of Contents and Provenance

There is enormous room for improvement here. "Voluntary" programs should be replaced with obligatory rules and regulations, backed by clear sanctions, to improve compliance and, critically, to prompt changes in behavior down through the ranks of the huge number

of firms involved in shipping to go beyond casual compliance and to take day-to-day vigilance seriously. Improvements in documentation of what is in the box and where it has been, however, can never overcome the fundamental problem: Contents are declared at the point of origin by whoever stuffs the box and are not really checked thereafter.

Personnel

The workforce that handles containers, less so the crane operators at ports than the short-haul truckers who haul the boxes from the ports to their first inland stop, can easily be penetrated by terrorists. The drivers are a particularly low-paid and high-turnover workforce. Efforts to establish a Transportation Worker Identification Credential, which would provide positive identification and background checks, have not yet been very successful.

Technology

The burden thus falls on technology—on the intelligent deployment of existing technologies and the rapid development of new and better technologies. Used in conjunction with one another, rather than as replacements for one another, they could provide an excellent, although regrettably still imperfect, security shield. There are several different kinds:

- **In-port radiography, or visualization machines**: These machines peer into the box and see if the contents correspond with what the manifest states the box contains: Is there a cylindrical steel object where there should be toys and tools? Is there anything anomalous? This implies rapid checking against electronic manifests that list contents and provenance. These machines are being installed at major U.S. ports; they should also be installed at ports of embarkation; many have been. Obligatory, not voluntary, screening before sailing, backed by strong penalties—such as a red lane, green lane system—should be imposed.
- **In-port passive radiation detection devices**: These devices detect radiation emitted by concealed radiation sources. They

are now being deployed on a large scale. They are relatively cheap to purchase and operate; critically, they are fast and do not impose delays. But they are very far from satisfactory in their capabilities; they cannot detect well-shielded dirty bombs and yield false positives when tuned to a sensitivity that can discern some shielded nuclear devices. (There is more normal radiation out there than one might first expect.) They should be replaced by a new generation of **active radiation detectors**. These will be much more expensive to install and operate and slower, too. Unfortunately, they do not yet exist in tested, deployable models. Research and development programs are under way, with many laboratories and producers competing, and deployable models should (it is hoped) begin to appear in a year or so.

- **In-box sensors:** These would operate all the time, in real time, and would be connected to receiving stations by radio frequency, to detect (passively) radioactivity, various chemicals, temperature, light, people, and, of course, tampering with the box and the sensor itself. They should be obligatory in all containers entering U.S. ports from abroad. Despite their vulnerabilities and shortcomings, if used in conjunction with the other layers of defense technology, they make penetration significantly more difficult.

Costs

Tracking technology is the one element in this multilayered system that will more than pay for itself in cost savings (lost and stolen containers) and in efficiency enhancement, although estimates on savings differ substantially. The other elements are net costs—for which estimates also vary considerably. The full, layered technology panoply defined above will cost billions of dollars. Is this a lot? A little? The cost should be compared with relevant metrics. Compared to the costs of the potential dangers the system seeks to prevent, the cost is small: A WMD in a major city defines true catastrophe. Compared to the costs of other defense systems, such as nuclear submarines or stealth aircraft fleets, the

numbers seem small. Compared with the value of the contents inside the shipping containers—half a trillion dollars in-bound—we are around 1 or 2 percent; substantial, but not overwhelming. Compared to trade measures being pressed on our Asian trading partners by the U.S. government, such as revaluations (increases) in the value of Asian currencies vis-à-vis the U.S. dollar, the costs are derisively small. Of course, it is an absolute "no-no" to discuss security costs imposed on imports in trade terms; it is a violation of both the spirit and the letter of basic international trade rules. But most sensible impositions of costs will have that effect. The costs (if not just assumed by the U.S. government) are passed to the supply chain, from Wal-Mart back through the manufacturer in Asia, and distributed by market power. They surely will be noticed by foreign companies and governments, even if necessarily dismissed by U.S. trade authorities, and unlike the case of many other trade measures, a significant proportion of higher security costs can translate directly into U.S. jobs.

Anticipated Results

Even if all these problems are resolved, and even if the active radiation detectors prove to be effective and robust, there is no guarantee whatever that tech-savvy terrorists will not succeed in slipping a weapon of mass destruction into the United States inside an in-bound container. But the full system will make that significantly more difficult and, it is hoped, significantly less likely. The chance of detecting and stopping conventional explosives from penetrating our defense and triggering highly destructive reactions is somewhat smaller, but abundant domestic sources of explosives provide a viable alternative to imports. And careful planning, rigorously applied, can contain the self-inflicted damages.

Finally, even if container security proves completely effective, it will not make America safe, not even from weapons of mass destruction entering from the sea. One can horrifically imagine, in vivid detail, a glorious oceangoing yacht sailing on a beautiful day into Miami, or Los Angeles, with bikini-clad fashion models and packs of photographers cavorting on deck: Scores of small sailboats circle, stare, and wave, while down below, someone sets off the nuke.

References

ABI Research, *RFID Border Security Markets,* Oyster Bay, New York, 2005.

Allison, Graham, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, Times Books, New York, 2004.

Austen, Jane, *Pride and Prejudice*, T. Egerton, London, 1813.

American Nuclear Society, *Sessions on Radiological Terrorism 2002,* Washington D.C., 2002.

American Shipper, "U.S. Customs Emphasizes Rapid Compliance with Advanced Manifest Rule," *American Shipper Online*, Vol. 6, No. 235, December 3, 2002, available at www.americanshipper.com.

Arquilla, John, "The Forever War," *San Francisco Chronicle*, January 9, 2005, p. 6.

Associated Press, "Authorities Find 32 Chinese Migrants in Ship Container at LA Port," *San Jose Mercury News*, January 16, 2005.

Balfour, Frederik, "Fakes!" *Business Week,* February 7, 2005, pp. 54–64.

BearingPoint, "A Secure Global Supply Chain: Evaluating the Return on Investment," McLean, Virginia, 2004.

Beckner, Christian, and Mark Shaheen, *Sensors and Homeland Security: A Market Assessment,* Civitas Group, Washington, D.C., 2005.

"Biological Terrorism," *The Economist,* May 24, 2005.

Bonner, Robert C., "Statement Before House Appropriations Committee, Subcommittee on Homeland Security," Washington, D.C., March 15, 2005.

Bowman, Michael, "Congress Told U.S. Port Security Improving, but Still Deficient," *Voice of America*, May 18, 2005, available at www.VOANews.com.

Bowman, Steven R., *Biological Weapons: A Primer,* CRS Report for Congress, RL31059, Congressional Research Service, Library of Congress, Washington, D.C., July 24, 2001.

"China's Manufacturers Sing Pearl River Delta Blues," *Taipei Times*, June 16, 2004.

Crist, Phillipe, *Security in Maritime Transport: Risk Factors and Economic Impact*, Maritime Transport Committee, Directorate for Science, Technology and Industry, Organization for Economic Cooperation and Development, Paris, July 2003.

Falk, Ophir, and Yaron Schwartz, "Terror at Sea: The Maritime Threat," Institute for Counter-Terrorism (ICT), Herzliya, Israel,

April 25, 2005, available at www.ict.org.il/articles/articledet.cfm?articleid=532 (as of August 5, 2005).
Federal Emergency Management Agency, *Are You Ready? A Guide to Citizen Preparedness,* Washington, D.C., September 2002.
Flynn, Stephen E., *America the Vulnerable: How Our Government Is Failing to Protect Us from Terrorism*, HarperCollins, New York, 2004.
Fortner, Brian, "Electronic Seals Track Containers to Improve Port Security," *Civil Engineering,* Vol. 72, No. 10, October 2002.
Frittelli, John F., *Port and Maritime Security: Background and Issues for Congress,* CRS Report for Congress, RL31733, Congressional Research Service, Library of Congress, Washington, D.C., December 5, 2003.
Frontline Solutions, *'Smart' Container Success Will Depend on Government Mandates,* Peterborough, New Hampshire, February 1, 2005.
Greenspan, Alan, "Committee on Financial Services Hearing," February 28, 2001.
Harrald, John R., Hugh W. Stephens, and Johann Rene van Dorp, "A Framework for Sustainable Port Security," *Journal of Homeland Security and Emergency Management,* Vol. 1, No. 2, 2004.
Harris, Shane, "Detecting the Threat," *Government Executive Magazine*, July 15, 2002.
Hasbrouck, Edward, "LaborTech Denounces Surveillance of Standards of Travelers and Transport Workers," April 8, 2004, available at www.labortech2004.org.
Haveman, Jon D., and David Hummels, *California's Global Gateways: Trends and Issues*, Public Policy Institute of California, San Francisco, California, 2004.
Herron, Kerry G., and Hank C. Jenkins-Smith, *Evolving Perceptions of Security*, University of New Mexico, Albuquerque, New Mexico, 1996.
Inbar, Daniel, and Michael Wolfe, *New Smart Container Studies Find: Deployment of Maritime Smart Containers Will Improve U.S. Economy and Profits as Well as Security,* Homeland Security Research Corporation and North River Consulting Group, San Jose, California, and North Marshfield, Massachusetts, April 2004.

Kates, Brian, "Harbor Fears High, Terror Funding Low," *New York Daily News*, December 21, 2003.
Knobler, Stacey L., Adel A. F. Mahmoud, and Leslie A. Pray, eds., *Biological Threats and Terrorism: Assessing the Science and Response Capabilities*, National Academies Press, Washington, D.C., 2002.
Krugman, Paul, "The Costs of Terrorism: What Do We Know?" presented at *The Nexus of Terrorism and WMDs: Developing a Consensus,* Princeton University, December 12–14, 2004.
Kurtz, Howard, "Terrorism Stunt Angers U.S. Officials," *Sydney Morning Herald*, September 13, 2003.
Lane, Earl, "Port Security: Concern Lingers Over New Scanners; Their Use Is Growing, But Whether They Can Detect Materials Used to Make Devasting Weapons Is a Worry," *Newsday,* August 17, 2004.
Lawler, Andrew, "The Unthinkable Becomes Real for a Horrified World; Research and Development to Combat Terrorism; Statistica Data Included," *Science*, Vol. 293, No. 5538, September 21, 2001, p. 2182.
Lipton, Eric, with Matthew L. Wald, "U.S. to Spend Billions More to Alter Security Systems," *New York Times*, May 8, 2005a.
Lipton, Eric, "Loopholes Seen in U.S. Efforts to Secure Overseas Ports," *New York Times*, May 25, 2005b.
"Looking for a Big Market? Try Container Security," Sunday Business via NewsEdge Corporation, June 3, 2005, available at securityinfowatch.com/article/article.jsp?id=4289&siteSection=384 (as of April 2, 2006).
Nacht, Michael, *Working Smarter, Faster, Safer: Technological Innovations and Adjusted Work Practices for Enhanced Security and Productivity at West Coast Ports,* Goldman School of Public Policy, University of California, Berkeley, California, October 26, 2001.
National Defense University, "Dirty Bombs Could Cause Devastating Economic Damage," available at http://www.ndu.edu/info/PressReleases/dirtyBombs.cfm (as of July 2005).
Nuclear Research Center, "Fact Sheet on Dirty Bombs," available at www.nrc.gov/reading-rm/doc-collelctions/fact-sheets/dirty-bombs.html (as of February 25, 2004).
Organisation for Economic Cooperation and Development, *Report on Container Transport Security Across Modes*, Paris, 2004.

Powell, Alvin, "New Harvard Report: Chilling Warnings on Nuclear Terror," *Harvard University Gazette,* March 20, 2003, available at www.news.harvard.edu/gazette/2003/03.20/11-warnings.html (as of April 2, 2006).

Rae Systems, *Securing the Supply Chain: Container Security and Sea Trial Demonstration Results,* Sunnyvale, California, January 2005.

*S*coville, Herbert, Jr., "The Neutron Bomb Makes Politics, Not War," *New York Times*, August 26, 1981.

Skinner, Richard L., "Statement of Richard L. Skinner, Acting Inspector General, U.S. Department of Homeland Security, Before The Committee on Commerce, Science, and Transportation, United States Senate," Washington, D.C., May 17, 2005.

Slovic, Paul, *The Perception of Risk*, Earthscan Publications, London, 2000.

Stern, Jessica, "The Prospect of Domestic Bioterrorism," *Emerging Infectious Diseases: The Journal of the Center for Disease Control,* Vol. 5, No. 4, July–August 1999.

U.S. Government Accountability Office, *Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges,* Statement of JayEtta Z. Hecker, Director, Physical Infrastructure Issues, Before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, U.S. House of Representatives, GAO-03-297, Washington, D.C., November 18, 2002.

U.S. Government Accountability Office, "Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers," Statement of Richard M. Stana, Director, Homeland Security and Justice, Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, U.S. House of Representatives, GAO-04-325T, Washington, D.C., December 16, 2003.

U.S. Government Accountability Office, *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security,* GAO-04-838, Washington, D.C., June 2004.

U.S. Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, "Global Spread of Chemical and Biological Weapons," Hearings, Washington, D.C., February 9–May 17, 1989.

Van de Voort, Maarten, Kevin A. O'Brien, Adnan Rahman, and Lorenzo Valeri, "*Seacurity:" Improving the Security of the Global Sea-Container Shipping System,* the RAND Corporation, MR-1695-JRC, Santa Monica, California, 2003.

Veiga, Alex, "Radiation Detectors to Scan All Incoming Cargo at LA Port Complex," *Associated Press,* June 4, 2005.

Wein, Lawrence M., Alex H. Wilkins, Manas Baveja, and Stephen E. Flynn, *Preventing the Importation of Illicit Nuclear Materials in Shipping Containers,* Stanford University and Council on Foreign Relations, Palo Alto, California, and New York, 2004.

Willis, Henry H., and David S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain*, the RAND Corporation, TR-214-RC, Santa Monica, California, 2004.

Wolfe, Michael, *Technology to Enhance Freight Transportation Security and Productivity, Appendix to: Freight Transportation Security and Productivity,* North River Consulting Group, North Marshfield, Massachusetts, 2002.

World Shipping Council, "Liner Shipping: Facts and Figures," Washington, D.C., n.d.

World Shipping Council, National Industrial Transportation League, National Customs Brokers and Forwarders Association of America, Inc., and the Retail Industry Leaders Association, *Petition before the United States Department of Homeland Security, Bureau of Customs and Border Protection for Reconsideration of Final Rule: Required Advance Electronic Presentation of Cargo Information*, RIN 1651-AA49, Washington, D.C., 2004.

Wrightson, Margaret T., "Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges," Testimony Before the Committee on Commerce, Science and Transportation, U.S. Senate, GAO-05-448T, Washington, D.C., May 17, 2005.

5. Harnessing a Trojan Horse: Aligning Security Investments with Commercial Trajectories in Cargo Container Shipping

Jay Stowsky
University of California, Berkeley

Introduction

Policy efforts to induce the private sector to improve the security of cargo container shipping will benefit from careful consideration of how such improvements can also enhance the economic efficiency of the typical shipping supply chain. Impolitic as it may be to observe, the fact is that a major terrorist attack on a U.S. port (perhaps from a shipping container) may never come. If it does, it may turn out to be a fairly isolated, albeit economically and psychologically devastating, event. In either case, a massive security investment not offset by a concurrent achievement of the largest possible social or economic benefit would represent a colossal missed opportunity—a waste of economic resources that could have been artfully invested to create technologies that were by nature dual-use, that is, valuable for both homeland security and commercial purposes.

This chapter characterizes the private sector's early response to the increased awareness of potential security threats to cargo container shipping that dawned in the wake of the terrorist attacks of September 11, 2001. It is motivated by the conviction that profit-seeking investments by private sector shippers, carriers, and port operators to enhance the efficiency of the global containerized supply chain may do more to prevent terrorist groups from using container shipping as a conveyer of weapons of mass destruction (WMD) than will investments

targeted at the outset specifically to the security threat. It is motivated, as well, by a belief that lack of due attention to the opportunities for dual-use technology development may impede the growth of the civilian economy and the competitive fortunes of American industry in international competition and do little to improve homeland security. Such a failure of attention would replicate one of the costliest aspects of America's involvement in the 40-year Cold War, when military-led technology development sometimes benefited the civilian economy but sometimes also distorted the country's economic and technological development with only negligible effects on the nation's security.[1]

The best opportunities for dual-use investment are in the area of improving the transparency of the global container supply chain. Technologies that make container tracking easier while making tampering or breaching the container harder are the most lucrative from a purely private sector perspective and thus have already attracted the lion's share of private investment. For both security and supply chain efficiency, the ideal system is one that enables interested parties (those with no malicious intent) to track the containers as they move from link to link in the system. Available Global Positioning System (GPS) and radio frequency identification (RFID) technology can already record snapshots of a container's journey, enabling human interrogators to check at key points along the way for evidence of tampering or even WMD. Both shippers and security officials have an interest in developing the capability to track containers continuously and in real time, but it would be imprudent to put off investments in existing technology that can already improve both efficiency and security to a significant extent.[2]

Such investments were already under way before the September 11 attacks for purely commercial reasons, although they were not being made as quickly or comprehensively as security officials would prefer. Through a judicious balance of standard setting and procurement, the federal government could encourage this trend without dampening market signals and without distorting the trajectory of technological

---

[1]Stowsky (2004).

[2]Flynn (2004).

development with too many security-specific performance requirements. History suggests that the wisest approach is for the government to let private sector solutions emerge in response to private sector problems and then to provide inducements for private suppliers to "spin on" commercial technology to security applications, rather than funding those applications directly with the hope (often more hype than hope) that commercial spinoffs will rapidly emerge in the opposite direction.

Investments that would enable the supply chain to operate through a terrorist attack, or to quickly recover from one, promise less immediate commercial benefit and so have attracted much less private investment. Yet this is an area where the potential for dual use is also great, even if the scope of the potential returns becomes clear only in retrospect. This is also an area of technological development where the federal government should be willing to invest more heavily, in partnership with private investors who will be able to appropriate some of the returns to such investments in supply chain resilience as a purely commercial matter and so should be willing to put a significant portion of their own funds at risk. The largest share of public-led investment should target research and technological development in the area of remote sensing of chemical, biological, radiological, and nuclear agents—an area fraught with technological and practical barriers, both of which have impeded and will continue to impede private sector investment. But it is also an area where a breakthrough could produce exceptionally dramatic returns, both commercially and in terms of homeland security.

Since the late 1970s, a security-centered approach to developing dual-use technology has not prevented superior, commercially derived versions of security technologies from reaching open global markets, where they quickly become accessible to allies and adversaries alike. Most homeland defense technology, especially information technology (IT), now has commercial roots, and these roots extend around the globe. It is impractical, if not impossible, to prevent these technologies from ever diffusing to potential enemies. Homeland security cannot depend, therefore, on how well a system of export and publication controls maintains exclusive access to any particular technology over time.

Moreover, homeland security research and development projects that are isolated from the demands of potential users in mainstream commercial markets are apt to produce dual-use technology that is inferior in quality and price to that which will be available commercially. This is the lesson of significant numbers of dual-use technologies developed during the Cold War—numerically controlled machine tools, very high-speed integrated circuits, artificial intelligence software, flat panel displays, intelligent transportation systems, and encryption. In each case, the United States sponsored military-specific versions of the underlying technology, which were eventually overtaken by less costly commercial applications of equivalent or superior quality and functionality.[3] In contrast, the involvement of military, intelligence, and homeland security agencies in an open and collaborative development process can actually enhance prospects for commercialization of dual-use technology. This is the lesson of several other technologies developed by the United States during the Cold War—solid-state transistors and integrated circuits, Very Large Scale Integrated (VLSI) circuits, and computer-aided design tools, semiconductor production equipment, and the Internet.[4]

How Has the Private Sector Responded to the Terrorist Threat to Shipping and Ports?

The term "supply chain" refers both to the dozens of discrete steps by which components, subassemblies, and finished goods travel from their point of manufacture to their point of sale and to the collection of companies involved in the conveyance of goods for use or sale by a specific company. Thus, to take one prominent example, one may speak of the giant retailer Wal-Mart's "supply chain" both to characterize the scores of companies involved in designing, producing, and transporting the goods that end up stocking the shelves of Wal-Mart's growing roster of outlets and also to describe the series of steps—lorry to container,

[3]Stowsky (2004).

[4]Stowsky (2004).

container to ship, ship to shore, truck or train to store—involved in getting them there.[5]

Viewing the supply chain not as a series of discrete steps carried out by independent agents but as a system susceptible to "management" has been an element of competitive strategy at least since the advent of the multidivisional corporation. Before the 1970s, U.S. corporations normally managed their supply chains either by making them internal (i.e., owning many or most of the entities involved in the process, thus creating the classic vertically integrated firm), or by warehousing stock and supplies as insurance against short-term supply chain disruptions over which they had no control. The management trend toward refocusing on a firm's core competencies, combined with radical organizational innovations pioneered by Toyota and other Japanese firms from the 1950s through the 1970s, changed all that. Most major retailers and manufacturers now contract with independent suppliers for much of what they make or sell, and most rely on their suppliers for "just-in-time" delivery of parts and products, rather than building up buffer stocks in costly warehouses. In effect, the supply chain is now the warehouse. But the consequent cost savings has carried with it a vastly increased vulnerability to supply chain disruptions in the form of everything from pirates to dock strikes to, now, terrorist attacks.[6]

Like most commercial firms in the first years after the September 11 attacks, companies in the cargo container shipping business initially assumed an attitude of "watch and wait" to form a clearer picture of the scope and scale of the new terrorist threat. Private spending for supply chain security increased but at a rate not dramatically inconsistent with a decade-long trend toward higher spending on security that began well before September 11. For the most part, the first post-September 11 expenditures purchased security technology that was already available off the shelf.

Subsequently, as new generations of security products and services have started to emerge from corporate and government labs, corporate boards have begun to view investments in security as a necessary form of

---

[5]Sheffy (2002); Lee and Wolfe (2003); Willis and Ortiz (2004).

[6]See also Cohen, Chapter 4 of this volume.

insurance against terrorism and other sources of operational instability and disruption. The mandates provided by the U.S. Maritime Transportation Security Act (MTSA) of 2002 and the International Maritime Organization's new International Ship and Port Facility Security Code are also compelling port operators, shippers, and carriers to take action.[7] As a result, new product and services markets for maritime and port security are coming into sharper focus, in terms of supply, demand, and overall size.

When one examines this still-developing market, a couple of characteristics stand out. First, the 2001 terrorist attacks did not generate a brand new market. Rather, they amplified and accelerated an ongoing "digital transformation" of cargo container shipping with respect to both security and supply chain management. Before September 11, advances in digital electronics hardware and software had already started to multiply the actual and potential interconnections among the dozens of players involved in cargo container shipping. Companies that had been content before to rely on separate vendors for security guards and surveillance cameras, electric fences, and electronic firewalls had already started to seek suppliers who could offer more integrated, end-to-end security solutions. Thus, a segment of the market had already started to consolidate in the form of new security services firms offering to integrate different security products and solutions. The main effect of the September 11 attacks was to accelerate this pre-existing trend.[8]

This turn of what was previously a set of stand-alone product markets into a single consolidated market for integrated, information-technology-based solutions to overall security and supply chain management is the key competitive dynamic driving the continued expansion of security spending in the maritime and port sector. As in all advanced technology markets characterized by network scale economies, commercial success, as measured by market share, may depend more on the size of a company's portfolio of complementary products and services than on the technical performance of the company's point-targeted

---

[7]See Haveman, Shatz, and Vilchis, Chapter 7 of this volume.

[8]Gerin (2004).

security solutions.[9] Companies with superior products may struggle against competitors with larger partner networks or against companies that already have a large established base of installed products and after-sales services.

The Coexistence of Successive Technology Generations

A second significant feature of this burgeoning market for port and maritime security technology is the extent to which the market is segmented into distinct but overlapping technological generations. To analyze the competitive dynamics of any particular product segment, one must first understand whether the product in question represents a mature technology, a technology just coming to market, or a technology still being tested in corporate, university, or government labs. The prospects for different technological generations might differ dramatically in response to different levels or styles of government regulation, for example. The main point to understand is that different generations of port and maritime security technology are installed simultaneously and will need to be able to interconnect and interoperate for the foreseeable future.

As noted above, the initial reaction of commercial shippers, suppliers, and port operators to the September 11 attacks was to expand purchases of security products and services that were already on the market or just coming to market before the terrorist attacks. These products constitute a first generation of maritime and port security technology and make up the majority of the sector's current installed technology base. First-generation security products include such things as metal detectors and handheld radiation detectors, building or area access control systems, and fingerprint recognition software.

As a consequence, a common desire among many commercial shippers, importers, suppliers, and port operators contemplating new security technology is for new products and services that will enable them to integrate the disparate technologies in their installed, first-generation

---

[9]Shapiro and Varian (1999).

product base. These represent a substantial sunk investment, and the ports and shippers are not in any rush to replace or entirely upgrade it. For companies and investors on the supply side of this market, first-generation technologies are a low risk but still profitable investment, offering a steady stream of revenue, although one that has passed its peak. These products are starting to be replaced, albeit gradually, as second-generation products and systems start to come to market.

Most of the second-generation maritime and port security services and products have been designed to offer a broader array of security solutions combined into one integrated package. They tend to consist of "suites" of services and functions based on technologies that were under development before September 11 but which may not have been offered commercially before the attacks. In some cases, these products represent the repurposing of technologies that were under development before September 11 but which had targeted other, sometimes non-security-related applications. As one would expect, many of them are designed to interconnect with first-generation applications so that suppliers do not have to try to overcome customer resistance to replacing an entire installed base of first-generation security products.

Second-generation products include screening or imaging technologies that can perceive plastic and ceramic explosive devices hidden in luggage or under clothing and various "smart surveillance" technologies that match images captured by security cameras to databases designed to trigger an alarm and further investigation. This is the generation of products that has probably benefited most from increased federal funding for new technology deployment, mainly in the form of pilot or demonstration projects such as the U.S. Department of Homeland Security's Operation Safe Commerce (OSC). This market segment is the site of considerable new venture development but also a great deal of acquisition activity, as larger, established security, logistics, and enterprise software suppliers attempt to keep up with the latest available product offerings.

Many firms selling products in this market have adopted a strategy that focuses on bundling their products with complementary products from other companies whose technologies aim at securing other points along the supply chain. Others are partnering with logistics companies

in an attempt to succeed as providers of integrated end-to-end security solutions. Consequently, this is a market where competition over the establishment of intellectual property rights and industry standards, which in some cases will require that customers replace installed equipment, will be tough. As suites of complementary products develop, in other words, competition in this sector is likely to center on contests between rival technology platforms.

Finally, breathless press accounts have focused much attention on the next or third-generation of port and maritime security technology—a set of products and services that still has not emerged from the research lab. This generation of technology is characterized by cutting-edge applications in developing fields such as nanotechnology that hold out the promise—but still only a promise—of dramatic leaps in both operational efficiency and security within and across the entire transportation supply chain. Some of this technology is just now beginning to be integrated into the most advanced versions of currently available security products and services.

This market segment is still dominated by privately held start-ups, many of which are rooted in university or government laboratories. They are focusing their research on areas where a breakthrough might be expected to create new capabilities across a broad range of security needs, for example, in the area of remote sensing equipment that might detect a wide range of potentially dangerous agents. This is the realm of applied research where technological breakthroughs might be expected to emerge, with either price or performance attributes improving dramatically enough to induce customers to abandon their loyalties to previous generations of security technology.

Other Factors Shaping the Private Sector Response

Besides the overall shift toward integrated rather than stand-alone solutions and the simultaneous presence of three generations of technology, the private sector response to security threats in the cargo container shipping sector is shaped by at least five additional factors. These include (1) the need for technical standards, (2) the "public goods" nature of investments in port and maritime security, (3) liability issues, (4) the tradeoff, embodied in many security products, between

security and other important societal values, particularly privacy, and (5) the extreme sensitivity of this market to unpredictable external events.

The Need for Standards

A typical shipment of cargo from point of origin to port of entry by container involves as many as 25 distinct organizations.[10] With some 25,000 containers arriving at U.S. docks each day, and tens of thousands traversing ports across the rest of the globe, the opportunities for theft, fraud, smuggling, and terrorist infiltration are enormous.

Current security solutions, such as electronic antitamper seals; chemical, radiological, and biological sensors; tracking technologies of various types; and encrypted data transmission, tend to secure the nodes of the supply network rather than providing true end-to-end security along the entire supply chain. To achieve the latter, industry and government agencies will have to agree on technical standards for interoperability and interconnection. Commercial suppliers, shippers, and port operators cannot afford to maintain multiple technical platforms, infrastructure, or communications protocols from the cargo suppliers' facilities all the way to the final receiving location.

So far the U.S. government has been relying mainly on industry self-regulation to bring about standardization. The shipper and carrier industries have been responsive, but only to a point. A regulated security system offers many benefits to commercial shippers and carriers, as it is likely to speed the movement of cargo more rapidly through the world's ports, freeing ships up more quickly for the next load. U.S. Customs and Border Protection (CBP), which incorporated parts of the Customs Service and is part of the U.S. Department of Homeland Security, has issued some new rules, most prominently a requirement that ocean carriers must file a manifest, electronically, 24 hours before a cargo container bound for the United States is loaded at a foreign port. But the U.S. government has wielded more carrots than sticks.

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary program that shippers and carriers can participate in to assure CBP that they have adopted best practices for the secure packing,

---

[10]Flynn (2004); Randy Koch (2004); Powell (2004).

tracking, and distribution of all goods and services bound for the United States. In return, CBP rewards C-TPAT qualified shippers and carriers with fewer inspections and expedited processing (a new ranking system grants the highest-ranked, or most secure, members only relatively infrequent random inspections).[11] Similarly, Operation Safe Commerce (OSC) is a publicly subsidized collaboration among shippers, carriers, and port operators at a small group of the most active U.S. ports to promote testing, evaluation, and fielding of container scanning and tracking technologies and best practices for the safe movement of containerized cargo.

Still, a number of essential process questions remain to be settled, by industry consensus, government mandates, or both: What are the minimum documents required for transmission and when? What baseline encryption standards are necessary at each point along the supply chain? What constitutes a security breach, and what types of exceptions are allowable? Who needs to report a security breach and to whom? What is the procedure to mitigate the risk of such breaches? Furthermore, when information on risk and security is shared between corporate entities and government agencies, questions of data ownership often arise. Who owns what data? With whom can the data be shared? Where should security profile data be stored—with individual shippers or federal agencies?

"Public Good" Aspects of Maritime and Port Security

Analysts have argued that the private sector will be willing to bear most of the cost of building a more terrorist-deterring system of maritime transportation because the resultant commercial benefits of improved inventory control and fast-track shipping will more than pay for the private costs of assisting the national security project. This may not be clear to any particular commercial firm before the fact, however. There are clearly incentives for firms to free ride on the investments of others, as they will benefit from systemwide increases in efficiency and security whether they pay for them or not.

---

[11] Bonner (2005).

Most cost estimates for cargo container security put the bill at around $500 per container;[12] carriers typically generate $100 of profit per use of each container (although many are reluctant to admit that they make any profit at all). In any case, many carriers claim not to generate enough revenue to pay for the new integrated security solutions up front (although, pressed to do so, they would no doubt pass as much of the cost onto their customers and suppliers as they could without driving away significant business). For the economic and security benefits of such investments to be realized, therefore, the industry will have to be induced to act collectively to establish the requisite standards and spread the costs among all of the potential beneficiaries. Without voluntary action by the private sector, the U.S. government may have to enact regulatory mandates, a fact that even many shippers and carriers have openly acknowledged.[13]

Moreover, for an individual firm or port, the added benefit from an investment in better container tracking is easier to measure (and thus easier to justify in terms of positive net present value) than is the extra value of investments in the system's overall capacity to operate through and after a terrorist attack. Just as the U.S. government may want to subsidize or accelerate investments in container shipping transparency that the industry was starting to make on its own before the September 11 attacks, it may want to focus its investment of public resources (in research and development, for example) on those areas of collective benefit that any individual firm might be harder pressed to justify. Investments to enhance the ability of the overall system of international containerized shipping to restart activity after an attack fall squarely in this category.

Liability Issues

As the cargo container shipping business starts to operate more like a vast computer-managed network, it will have to come to grips with some

---

[12]Flynn (2004); Lok (2004). In his interview with Lok, Flynn breaks these costs into equipment that monitors the position and integrity of the cargo, chemical sensors, radiological sensors, and biological agent sensors, although the existing biological agent sensors as of 2004 were not yet affordable or dependable enough for commercial use.

[13]Christopher Koch (2004); Powell (2004).

of the same information security challenges that have made overall IT security so difficult to achieve in the Internet age.[14] One of these challenges is the creation of incentives for the private sector to invest in security products and procedures by assigning liability for security failures to the companies best positioned to avoid them. As it stands, no one entity is accountable for security breaches anywhere along the supply chain. With more than two dozen parties involved in a typical end-to-end shipment, such clear assignment of responsibility is unlikely to occur without government intervention or the concerted action of market leaders; the best candidates for that role would probably be the logistics companies currently campaigning to provide integrated security and supply chain solutions to shippers, carriers, and ports (and intermodal solutions encompassing trucking and rail as well).

The fundamental economic principle here is that liability should be assigned to the party that can do the best job of managing the inherent risks. Careful analyses must be done to locate the weak points in the overall supply chain, from point of origin to final destination. At each point a different party might be best positioned to strengthen it. The need is to create the appropriate risk management incentives by assigning liability for security breaches to the parties best equipped, at each stage, to control the risk.

Once this is accomplished, shippers, carriers, port operators, or systems integrators will want to insure themselves against the risks for which they are liable. Insurers, who are only beginning to serve this market, will then have an incentive to alert their clients to industry best practices. This may be the easiest way to create a vibrant market for new maritime security technology, as companies compete to get their products (or integrated product suites) certified by insurers who will then give their clients reduced rates for installing them. This process will not become self-sustaining, however, unless legal liability is clearly assigned to responsible parties at each point of the supply chain.

---

[14]Varian (2000).

Tradeoffs Between Security and Other Societal Values

Many of the tracking, screening, and surveillance technologies proposed (or already in use) for securing port facilities and container shipping could require a sacrifice of individual privacy or subject innocent individuals to various forms of profiling—ethnic, racial, and otherwise. Both of these concerns have already caused some consumer resistance to the deployment and continued development of certain security technologies. In addition, some civil liberties activists have campaigned for restrictions on the permissible range of use of the new technologies; this could stifle technological innovation unnecessarily.

The concerns of consumers and civil libertarians are not without basis, however. For example, the standardized radio frequency identification chips that are on track to replace the familiar Universal Product Code (UPC) bar codes on all manner of products and shipping containers can be hidden from sight, as can the devices that read them. Various proposals to require consumer notification when the chips or readers are present in products, stores, or public places have been resisted by retailers. So have proposals that consumers be given the right (as well as the ability) to remove or deactivate the tags at will. Industry groups have developed guidelines about the use of RFID technology, but they are voluntary.[15]

The dilemma here is a common one with respect to all of the new digital security technologies. Use restrictions such as those that have been proposed for RFID devices would be frustrating (and in some cases costly) but not fatal to widespread commercial adoption of the technology. Yet much of the private response by industry to even the most reasonable expressions of concern has been so dismissive that it has had the effect of pushing more people into the arms of those who would prefer to hobble or prevent deployment of the technology altogether. Aside from the commercial efficiency benefits forgone, this attitude could undermine security efforts at many levels, not just efforts to help prevent terrorist attacks (for example, the installation of RFID chips in car keys, smart cards, and steering columns can help to prevent auto theft).

---

[15]Garfinkel (2004).

There are, however, some areas of real divergence between the wishes of security officials and the needs of commercial retailers. Whereas commercial interests probably could live with a regulatory regime that enabled consumers to know when tracking devices (chips and readers) are present, and even with a regime that would enable consumers to deactivate them at will, security officials are not likely to want to so weaken the capabilities that these new technologies afford them. Security officials and civil libertarians should be encouraged to create a forum for mutually assessing and balancing the tradeoffs implied by the use of these new devices for homeland security purposes.

The Special Sensitivity of the Security Market to Terrorist Events

The use of hijacked commercial airplanes by the September 11 terrorists understandably focused the attention of U.S. government officials on aviation security. Legislation to improve security at ports was introduced but funded at levels significantly below what would be needed to make the system of cargo container shipping even reasonably safe. Bills to expand funding for railway security were similarly underfunded or stalled in the first years after the September 11 attacks, despite their clear vulnerability to assault. This changed on March 11, 2004, with the devastating railway bombings in Madrid, Spain. Within weeks, the U.S. Congress had appropriated an additional $100 million in railway security grants for fiscal year 2005. Any analysis of the private sector response to the security threat at ports and on the high seas should allow for the possibility that a successful terrorist attack via cargo container would significantly reshape expectations on both the demand and supply side of the security product and services market.

Key Technologies

The increasing pervasiveness and declining cost of digital technologies has made it possible, as never before, for any company to view its supply chain as an interconnected system, subject to cost and quality control. Manufactured goods and their components can be represented as digitized data points and tracked as data are passed from point to point along the supply chain. By subjecting manufactured

goods and their components to near-constant surveillance and tracking (tracking the goods themselves, the containers in which they are shipped, or the ships and trains and trucks on which they are moved), companies can rectify or guard against all kinds of losses from theft, weather, accidents, or other adverse events. By adding various sensor, screening, and antitamper technologies to the mix, carriers and ports can also help prevent the malicious use of their shipping containers to transport terrorist weapons of mass destruction.

Six key technologies cut across the markets for improved security and supply chain management at ports and in the cargo container shipping industry. They are (1) sensor technologies, (2) identification and authentication technologies, (3) screening technologies, (4) surveillance technologies, (5) antitamper, tracking, and inspection technologies, and (6) integrated solution and data analysis technologies.

Sensor Technologies

A great deal of scientific attention is focused on the development of new generations of sensors to detect chemical, biological, radiological, or nuclear weapons of mass destruction, any of which would otherwise be relatively easy to conceal aboard a cargo container. But sensors able to detect any of these agents in the form and at the scale at which they would need to be detected to secure a port (or to prevent the transport of WMD inland by truck or train) do not exist. Furthermore, the development of such sensors constitutes an enormous scientific and technological challenge. With respect to radiation, for example, all sorts of objects, from bananas to ceramic tiles, emit harmless radiation naturally and would need to be distinguished from devices loaded maliciously onto container ships by groups or individuals aiming to cause harm.

Because remote sensors with the capabilities described would be breakthrough technologies for homeland security, efforts to create them are heavily concentrated in government laboratories. For private investors willing to bear the risk, the payoff of the successful development of a deployable multithreat sensor technology would be

exceptional.[16] In addition, such sensors represent a major opportunity for the creation of dual-use technology, as they would be useful for the rapid identification and containment of accidental or naturally occurring releases of biological, chemical, or radiological agents into the atmosphere near industrial facilities, for example, or in emergency rooms. With respect to cargo container shipping, however, sensors are not perceived to have many uses beyond their essential security role; they will not enhance supply chain efficiency, although they might be useful in helping to get supply chains up and running more quickly after an attack if they can be used to reassure people that cargo and facilities are safe.

Identification and Authentication Technologies

Much private sector research and development is focused on technologies that would be used to identify and authenticate individuals who come into contact with cargo containers, from those who stuff the boxes to those who unload them at their final destination. Such technologies include increasingly familiar products such as smart cards that include optical memory and biometric capabilities such as iris scanning and facial recognition. Private companies and government agencies have already been using such technologies for some time to identify their employees and to permit their entry (and in some cases exit) from the workplace.[17] The issue of tracking when an employee exits the workplace (the loading dock, for instance) as well as when he or she enters has been a matter of some contention.

Other contentious issues in this regard include the high potential for false positive rates, particularly with the use of immature technologies such as facial recognition systems. The extent to which high false positive rates cause significant supply chain delays, however, depends as much on the human systems put in place to deal with positive readings as it does on the capabilities of the current generation of technology.

---

[16]Vendors developing remote sensors include Alexeter Technologies, CombiMatrix, Cepheid, MesoSystems Technology, Nanosphere, and Universal Detection Technology.

[17]Vendors in this category include A4 Vision, Acsys Biometrics, ActivCard, Bioscrypt, ChoicePoint, Cross Match Technologies, Digimarc, Drexler Technology, Identix, LG, Motorola, NEC, SAGEM, Schlumberger, and Viisage.

More difficult to solve may be the need for significant back-end infrastructure to store data against which various physical identifiers can be matched. The potential civil liberties implications of any centralized warehousing of these biometric data are likely to raise significant obstacles to the widespread deployment of technology designed in this particular form, especially those linked to DNA sampling.

Screening Technologies

In the area of screening technologies, work currently is focused on two issues. First, there is the issue of reducing the costs of screening cargo containers by increasing cycle time or throughput. This is a particularly pressing concern for ports and represents the major tradeoff between enhanced security and improved efficiency from advances in transparency (tracking) along the supply chain. Container screening adds time to the processing of containers; port operators or customs inspectors must also bear the significant cost of the scanning equipment. Current leading technologies for screening cargo containers include x-ray and radiological/nuclear screening systems and systems geared to explosive and explosive trace detection.[18]

The research emphasis in screening technology is in the area of so-called "smart screening" systems. The idea here is to arm the screening machines with software that can detect anomalies and then automatically alert human operators to the need for further inspection and, perhaps, the need to instigate countermeasures. Vendors would like to improve the efficiency of screening machines by making them more broadly effective across the entire range of threatening agents, which include chemical, biological, radiological, and nuclear (CBRN) weapons. Screening machines are likely to incorporate advanced sensors to detect these and other potential threats, including new types of explosives.

Scanning equipment is expected to enhance security by enabling the detection of weapons at ports of entry, thereby preventing their transport onto the mainland by truck or train. The expectation is that better screening technologies will also reduce commercial losses from fraud by

---

[18]Vendors in this category include American Science and Engineering, InVision (General Electric), L-3 Technologies, OSI Systems, SAIC, and Smiths Detection.

enabling the quicker detection of illegal or dangerous goods and their removal from the supply chain.

Surveillance Technologies

Surveillance technologies are among the most controversial of the products being marketed to achieve better security, particularly in large urban areas where they are being deployed to cover larger and larger areas, such as Times Square in New York City or the National Mall in Washington, D.C. Established surveillance technologies include infrared and motion detection camera systems and monitoring systems designed for radiological detection. These technologies are already being installed at ports to help detect unusual or unexplained activity or suspicious objects on the docks. As the July 2005 bombings of the London bus and subway system suggest, these technologies may not be particularly useful for deterring suicide attacks, but they may prove invaluable for diagnosing the nature of an attack in progress or for investigating the source of an attack once it has occurred.

New generation "smart surveillance" technologies incorporate software that can flag anomalous activity and alert human operators to the need for further inspection. Current research is aimed at the even more controversial objective of linking systems of surveillance to databases stocked with information on dangerous individuals or on characteristics of behavior, demeanor, and appearance thought to be suspicious or associated with malicious intent.[19]

Antitamper Seals and Tracking and Inspection Technologies

A new class of electronic seals is being affixed to the main latch of most cargo shipping containers.[20] These seals serve as RFID devices, automatically signaling the container's location as it passes fixed points outfitted with tag readers along the supply chain (for example, loading cranes and port gates). Moreover, the newest tags come equipped with

---

[19]Vendors in this category include CRS Technologies, InteliTrac, NEC, Northrop Grumman, ObjectVideo, and Vistascape.

[20]Commercial vendors working on this segment of the shipping security product market include Savi Technology, NaviTag Technologies, and IsoTag.

intrusion detection technology. There is a magnetic field around each seal, and interruptions are recorded on a memory chip that notes the time of the event. So-called "smart" containers, currently under development, will go further, using on-board sensors to detect radiation or chemical residue but also light and pressure changes that might indicate that someone has attempted to cut or drill an opening through the side of the box. These anomalies would then either sound an immediate alarm or get picked up the next time the container passes a tag reader, alerting human operators to the need for further inspection.

Private sector competition has driven the adoption of technologies for tracking goods as they move through the supply chain, including RFID, bar-coding, GPS, and Wi-Fi.[21] The expectation is that tracking will render the supply chain more transparent, enabling both shippers and carriers to pinpoint the location of their goods anywhere in the shipping sequence from port of origin to final destination. From a commercial standpoint, the major objective is to be able to rapidly locate bottlenecks if and when they occur so that shipping routes can be redirected and optimized.

From a security standpoint, the ideal system would enable continuous communication and tracking. This can be accomplished if seals are connected to transponders that can exchange signals with orbital satellites. This sort of continuous real-time communication will be quite expensive, however; this is one area where security needs may diverge from the needs of most customers in the commercial marketplace. The exceptions to this will probably be for cargo that is itself high risk (such as explosive chemicals) or high value. For these types of shipments, the desires of government security agents may match the investment incentives of commercial shippers.

Enhanced tracking promises other commercial advantages; it can assist in the early identification of damaged, misrouted, or unapproved goods, reducing losses from both shipping damage and fraud. More so than the other technologies discussed in the context of maritime and port

---

[21]Vendors in this category include Alien Technology, Intermec, Matrics Technology, Qualcomm, Savi Technology, Symbol Technologies, TransCore, and Zebra Technologies.

security, tracking technology can also help to mitigate the negative effect of supply chain disruptions by giving shippers and carriers an added capability to quickly locate shipments en route and then reroute them around major breaks.

For security officials, the use of tracking technology to verify goods as they move through the supply chain is expected to be a major tool for preventing the transport of weapons of mass destruction via cargo container. But technology does not currently exist with the ability to detect what is generally regarded as the greatest threat for transport via cargo container: a nuclear weapon or a radioactive, so-called "dirty bomb." There is still no technological substitute for good security procedures and well-trained human inspectors. But technology can help. Laboratory scientists are currently developing gamma ray detectors equipped with imaging components that can reveal the shape of materials that are emitting radioactivity from inside the box. But the technology is not yet refined enough to prevent economically unacceptable numbers of false positive readings from innocent materials such as ceramic tile that naturally emit small amounts of radiation.

Tracking technology presents a key opportunity for dual-use investment by the public and private sectors. Attention will need to be paid to the points at which security demands exceed the performance needs (and thus the investment justification) of commercial shippers. Too much reliance on security-driven investment might lead to the development of technology that is more specialized and expensive than commercial shippers, carriers, or port operators will be willing to install. (Willing, or perhaps able—it has been estimated that the security community's dream of outfitting key points, such as border crossings, along the transportation route supply chain with gamma ray sensors might cost as much as $10 billion.) So this is a technology area where the distance between security and commercial needs for development and deployment will have to be carefully calibrated and the mix of public-private investment arranged accordingly.

Integrated Solution and Data Analysis Technologies

As described above, the market for shipping and port security technology has evolved from a market for stand-alone product solutions

for security issues at specific points along the supply chain, to an integrated system and services market in which companies compete to offer holistic end-to-end security solutions that also promise to enhance the efficiency (i.e., profitability) of the entire supply chain network. Not only does a typical end-to-end shipment involve two dozen or more separate parties or organizations. It also involves 35 to 40 separate shipping documents. For a ship carrying, say, 3,000 containers, this would mean more than 100,000 separate documents that would have to be managed and secured in some way.[22]

The foundation of such systems and services includes an array of data mining and access control technologies that propose to help human intelligence personnel see patterns or "connect dots" that would normally be obscured in the daily blizzard of data and communications. These technologies are a focus of development in the private sector and also in the public sector, despite their having caused a major uproar in the context of the U.S. Defense Department's aborted Total Information Awareness (TIA) program.[23]

This market is certain to develop as companies engaged in cargo container shipping and port operations struggle to manage the proliferation of security products described in this chapter. Particularly challenging will be the need for vendors who can aggregate and integrate point security solutions of both different vendors and different technology generations, as managers will be resistant, because of sunk costs, to completely abandon security systems built up piecemeal over the years, no matter how seamless and turnkey the available solutions become.[24]

Most important, again, the extent to which private sector participants invest in new integrated security solutions on their own will

---

[22]U.S. General Accounting Ofice (2003); Lee and Wolfe (2003); Scalet (2003); Willis and Ortiz (2004).

[23]Stowsky (2004). Vendors in this category include BAE Systems, Boeing, Computer Sciences Corporation, General Dynamics (Veridian), Lockheed Martin, Northrop Grumman, Raytheon, and Verint Systems.

[24] Companies attempting to develop and provide integrated security solutions for maritime and port security include Unisys, Computer Associates, Allergent Technology Group, Hewlett Packard, and IBM.

depend critically on the extent to which these solutions also enable them to aggregate and analyze data on cargo in transit. This is what will enable them to use these systems to enhance supply chain efficiency and thus improve the bottom line. The dilemma is that this same information might be considered highly sensitive from an intelligence or law enforcement perspective—this makes resolution of the data ownership and information-sharing protocols even more urgent.

Conclusions and Policy Recommendations

Technologies that can make cargo container shipping more secure already exist and are available off the shelf, or nearly so. The technologies that can track the containers as they move from link to link in the supply chain are the same technologies that private sector shippers, carriers, and port operators were already pursuing before September 11, 2001, to improve the efficiency of their supply chain operations. A key policy objective now should be to allow these companies to continue to make the investments that they would want to make anyway for their own profit-seeking reasons.

Can the agencies responsible for port security gain access to the most promising dual-use technology from researchers at universities and commercial enterprises, yet still maintain a technological edge over opponents who have access to the same technology? They can if they focus more of their own investment spending on the front-end activities of basic research and exploratory development, where projects focus on investigating and advancing a technology's general state-of-the-art capabilities. And they should focus more internal resources on technology adoption and insertion, so that contractors are rewarded for quicker absorption of commercial technology in their security systems.

The first change will attract more participation from leading research universities and commercial firms, particularly when they are permitted to control the intellectual property that results. The second change depends on whether the U.S. Department of Homeland Security adopts procurement practices that encourage program officers to buy commercial technology off the shelf. In this environment, the underlying technologies are not secret, but security applications—systems architectures—can be. The point is to resist the tendency to

specialize for security applications as long as possible and also to adopt commercial technology for use in security systems as quickly as possible, more rapidly than potential opponents can.

Third, these research and development (R&D) policies must be rooted in a realistic appreciation of the extent to which security technology now derives from a global commercial technology base. This will require an acknowledgment by all governments that there are likely to be commercial sales of sensitive items outside their country of origin. Better tracking procedures will be required to assess what kinds of technology are already widely available in world markets. Nations that manufacture but wish to constrain the export of these sensitive items will need to conclude stronger export control agreements.

A shift toward more reliance on external R&D places commercial producers and research universities, as well as foreign nationals, at the center of the U.S. security apparatus. This obviously creates significant new security challenges for the United States. But, in a global economy, policies aimed at restricting participation in technology development and keeping the results secret are counterproductive. Commercial producers in excluded countries will find alternative technology sources and will, when they can, invest to develop the technologies themselves. The fact that many of these technologies (and much of the information about them) can be digitized and disseminated electronically means that their propagation will be increasingly difficult to monitor and control. In the digital age, the best approach to conducting security centered R&D is an approach that embraces openness.

A second objective would be to create market-based incentives to get these companies to internalize the costs of improving security all along the supply chain. This is a classic negative externality. The transformation of ships into floating warehouses, a consequence of just-in-time manufacturing strategies, combined with the digital transformation of supply chain management, has also rendered economies more vulnerable to terrorist disruption.

There are areas where security and commercial objectives conflict. It is essential to exploit opportunities for public-private collaboration to leverage emerging technologies for multiple uses (that is, both commercial and security applications). It is essential, as well, that such

collaboration be structured in such a way that market signals (and the trajectory of technological development) are not unduly distorted by desires from security officials for expensive bells and whistles that really are not essential for improving security. The effect on supply chain security may be negligible, but the effect on supply chain efficiency may be quite damaging if overspecialized security demands render some of this new technology too complex and expensive for commercial use.

Another possibility is that U.S.-based companies, more likely than their counterparts in Asia or Europe to win technology development contracts from the U.S. Department of Homeland Security, will end up being disadvantaged in international competition as shippers, carriers, and port operators start to prefer less-expensive, more commercially relevant products offered by foreign suppliers. This will create new headaches for U.S. security officials, with effects that could clearly spill over to negotiations involving the removal of restrictions on international trade.

In the end, as was often the case in the latter decades of the Cold War, simpler commercial technology may prove more effective and less expensive for security applications, when it is allowed to "spin on" to those applications, than reliance on technologies developed from their inception with specialized security needs in mind. From the standpoint of American homeland security officials, it would no doubt be preferable for that commercially developed spin-on technology to come from suppliers based in the United States.

References

Bonner, Robert C., "Statement of Robert C. Bonner, Commissioner, U.S. Customs and Border Protection, Hearing Before the Permanent Subcommittee on Investigations, Senate Committee on Homeland Security and Governmental Affairs," Washington, D.C., May 26, 2005.

Flynn, Stephen E., *America the Vulnerable: How Our Government Is Failing to Protect Us from Terrorism,* HarperCollins Publishers, New York, New York, 2004.

Garfinkel, Simson, "RFID Rights," *Technology Review*, November 3, 2004.

Gerin, Roseanne, "Security Opens New Doors: Guarding Nation's Ports and Commerce Sparks Growing IT Market," *Washington Technology,* September 13, 2004.
Koch, Christopher, "Remarks before the Journal of Commerce's 4th Annual Trans-Pacific Maritime Conference," Long Beach, California, March 9, 2004.
Koch, Randy, *Secure Commerce: Securing Your Global Supply Chain,* Unisys White Paper, Unisys Corporation, Blue Bell, Pennsylvania, 2004.
Lee, Hau L., and Michael Wolfe, "Supply Chain Security Without Tears," *Supply Chain Management Review*, January 1, 2003.
Lok, Corie, "Cargo Security," *Technology Review*, June 2004.
Powell, Peter H., Sr., "Testimony Before the Subcommittee on Trade of the House Committee on Ways and Means," Washington, D.C., June 15, 2004.
Scalet, Sarah D., "Sea Change," *CSO Magazine,* September 2003.
Shapiro, Carl, and Hal Varian, *Information Rules,* Harvard Business School Press, Cambridge, Massachusetts, 1999.
Sheffy, Yossi, "Supply Chain Management," *Defense Transportation Journal*, Vol. 58, September/October 2002.
Stowsky, Jay, "Secrets to Shield or Share? New Dilemma for Military R&D Policy in the Digital Age," *Research Policy*, Vol. 33, No. 2, March 2004.
U.S. General Accounting Office, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors,* GAO-03-770, Washington, D.C., 2003.
Varian, Hal, "Managing Online Security Risks," *New York Times,* June 1, 2000.
Willis, Henry H., and David S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain,* the RAND Corporation, TR-214-RC, Santa Monica, California, 2004.

6. Governance Challenges in Port Security: A Case Study of Emergency Response Capabilities at the Ports of Los Angeles and Long Beach

Amy B. Zegart
University of California, Los Angeles

Matthew C. Hipp and Seth K. Jacobson
Riordan Institute for Urban Homeland Security

Introduction

The governance challenges to implementing an effective port security strategy are daunting. Port security issues cross many levels of government, vary in important aspects from one port to the next, and require the involvement of many in the public and private sector who are unfamiliar with national security issues and unaccustomed to working together. What are the critical political, organizational, conceptual, and logistical problems for port security? Why do they exist? How can they be addressed? These are the major questions we ask.

We first addressed these issues in 2003, when with two other researchers from the UCLA School of Public Affairs we conducted a study of emergency response planning and preparedness at the Port of Los Angeles and the Port of Long Beach.[1] These two ports were selected for three reasons. First, the two adjacent ports, which share the same harbor, were the two busiest container ports in the United States;

[1] See Allen et al. (2003).

together, they constituted the third-busiest container port complex in the world.[2] The complex handled nearly half of all shipping containers entering the country—more than all of the ports on the East Coast *combined*—and carried more than $200 billion in containerized cargo annually.[3] As a result of their critical economic importance, the ports of Los Angeles and Long Beach had been recognized as among the most likely and most inviting terrorist targets in California. In a list of the top 624 terrorist targets in California released by the California Attorney General's Office in February 2003, the Port of Long Beach ranked third and the Port of Los Angeles ranked sixth.[4] A second reason for the ports' selection was the fact that federal officials frequently highlighted the Los Angeles region as a national leader in developing innovative ideas and processes for emergency response and counterterrorism. We thought it likely that the region would be ahead of the curve on port security issues as well and could offer valuable lessons for ports across the nation. Third and finally, UCLA's close proximity to the complex allowed our research team to gain personal, long-term access to key stakeholders—a factor we considered critical to successful analysis.

To gain analytic traction on the broad topic of port security, we narrowed our focus to issues that local leaders had the responsibility and power to address. Thus, intelligence and threat detection, which primarily involve the federal government, were not included. Similarly, programs such as the Container Security Initiative and the Customs-Trade Partnership Against Terrorism (C-TPAT), although critical components of a comprehensive port security strategy, fell outside the scope of the study. Our search for low-hanging fruit to improve port security at the local level quickly narrowed the range of potential issues to emergency response.[5] As we discuss in greater detail below, even these issues turned out to be far less easy to fix than initially expected.

---

[2]Although the Port of Los Angeles and the Port of Long Beach continue to be the busiest and second-busiest container ports in the United States, they are now the fifth-busiest container port complex in the world.

[3]Neffenger (2005).

[4]Hymon (2003).

[5]We have adopted a definition of "emergency response" similar to that discussed in Drabek and Hoetmer (1991), which defines the response phase of emergency

Our 2003 report identified two broad classes of governance problems that hindered efficient and effective emergency response at the port complex. The first was organizational: Responsibility for port security was highly fragmented, spanning two large cities, involving both the public and private sectors, and cutting across 15 federal, state, and local agencies with no single person or office in charge. The second challenge was conceptual: Emergency response plans were developed from past experience with natural disasters, which assumed that first responders could reach the port complex easily from surrounding areas. In a terrorist attack, however, the potential for mass panic, coupled with the port's limited geographic access by land routes, would likely delay first response significantly. Rather than using traditional emergency response models, local leaders needed to consider new approaches, such as training civilians to be their own first responders in vulnerable target areas.

Below, we provide a "10,000-mile check-up" of the 2003 study, highlighting the governance problems identified in the initial report, tracing what happened to the recommended fixes for each problem, and identifying the obstacles and key success factors the project encountered.

Organizational Challenges

Background

Coordination and political oversight of emergency response efforts are never easy; success requires planning for uncertainty, fast action in moments of crisis, and operations that almost always cross agency lines. Since the 1970s, Southern California's first response agencies have led the nation in both developing and strengthening models for effective interagency incident management. However, we found coordination and oversight of emergency response efforts in port security to be problematic, with the Los Angeles/Long Beach port complex facing the toughest organizational challenges of any major port in the country.

---

management as those "actions taken immediately before, during, or directly after an emergency occurs, to save lives, minimize damage to property, and enhance the effectiveness of recovery."

The most serious impediment to effective coordination and oversight had to do with the particular political realities of the Los Angeles/Long Beach port complex itself. Although the two ports are geographically one place—they share the same harbor, the same roadways, and the same workforce—they are fierce business competitors and separate political entities. The two ports operate with separate management structures, separate police departments, and separate fire departments. They answer to different mayors and different city councils. In total, no fewer than 15 different agencies from five different political jurisdictions bear some direct responsibility for security and emergency management at the port complex (Table 6.1). Because of the size, structure, and multijurisdictional nature of the port complex, it is likely that numerous agencies would respond to a terrorist attack and that these agencies would be poorly positioned to work effectively together. As a result, it may be difficult to achieve coherent and effective command of an incident at the port complex even with established guidelines.

Such guidelines, we found, do exist, but they do not establish clear lines of authority or responsibility for emergency response. Federal law leaves unclear exactly who is responsible for port security. Section 102 of the Maritime Transportation Security Act directs the U.S. Coast Guard to develop Area Maritime Transportation Security Plans for both port security and emergency response at all domestic ports and requires the designation of a Federal Maritime Security Coordinator for each area.[6] The president has designated the Secretary of Homeland Security as "the principal Federal official for domestic incident management."[7] Yet the same directive recognizes that the initial responsibility for responding to a terrorist incident will likely fall on state or local authorities and gives lead responsibility for criminal investigations of terrorist acts to the U.S. Attorney General.[8]

---

[6]Maritime Transportation Security Act (2002). The Coast Guard has designated each Coast Guard Captain of the Port as the Federal Maritime Security Coordinator for his respective zone, "including all ports and areas located therein." 33 C.F.R. Part 103.200.

[7]Homeland Security Presidential Directive (2003).

[8]Homeland Security Presidential Directive (2003).

Table 6.1

Agencies, and Their Political Jurisdictions, Responsible for Port Security at the Los Angeles/Long Beach Port Complex

Federal
U.S. Coast Guard
Federal Bureau of Investigation
Transportation Security Administration
Maritime Administration
Central Intelligence Agency
Bureau of Alcohol, Tobacco, and Firearms
Bureau of Customs and Border Protection
Bureau of Immigrations and Customs Enforcement
Drug Enforcement Agency
State
California Highway Patrol
California State Lands Commission
County
Los Angeles Sheriff's Department
Los Angeles County Fire Department
Local
Los Angeles Police Department
Los Angeles Port Police Department
Los Angeles Fire Department
Long Beach Police Department
Port of Long Beach Harbor Patrol
Long Beach Fire Department

SOURCES: U.S. Coast Guard and analysis by authors.

State and local laws, which naturally differ across the country, do not elucidate the issue either. In California, the "Standardized Emergency Management System" establishes guidelines that require the use of the Incident Command System during multiagency and multijurisdiction emergency response. Local governments must follow these state guidelines to be eligible for reimbursement for response-related personnel

costs.[9] Under the Incident Command System, the agency overseeing emergency operations differs, depending on the nature and location of the event. During a multijurisdictional event, agencies establish a "Unified Command" where agency managers share decisionmaking responsibility within a group.[10] There is no formal leader. Individual agencies maintain operational control and responsibility for their own assets and personnel, and agency leaders are supposed to act cooperatively, transferring decisionmaking authority within the Unified Command group, based on changes in the nature of an incident.[11]

In other words, the Incident Command System offers flexibility but at the cost of confusion. Although the system allows agencies to adapt to changing situations by avoiding a rigid organizational structure, its effectiveness hinges on informal trust, cooperation, and institutional knowledge about which agency leads under what circumstances. No single individual or agency has the authority to make decisions and be held accountable for the results. Instead, when it comes to planning for and responding to disasters at the port complex, the buck appears to stop nowhere.[12] In our interviews, several port security officials expressed concern that these ambiguities in federal and state guidelines, coupled with natural bureaucratic rivalries, posed a risk of coordination breakdowns during a response to an incident at the port. As Captain Peter Neffenger, U.S. Coast Guard Captain of the Port for the Los Angeles–Long Beach port complex, explains, "Despite all of our years of working together, we are not as proficient as we should be at large

---

[9]Adam Sutkus, Director, California Governor's Office on Service and Volunteerism, telephone interview with Seth Jacobson, March 16, 2003. See also California Office of Emergency Services (1998).

[10]Adam Sutkus, Director, California Governor's Office on Service and Volunteerism, telephone interview with Seth Jacobson, March 16, 2003.

[11]For more information on the ICS, see Stumpf (2005).

[12]It is important to note that although the Incident Command System does not solve the dilemma of determining who is responsible for port security, emergency response agencies generally speak quite highly of it. In fact, the federal government has adopted the system as part of the National Incident Management System and, beginning in fiscal year 2005, began conditioning federal grants to state and local agencies on their adoption of the Incident Command System. Homeland Security Presidential Directive (2003).

multiagency, multijurisdiction responses. Just because you're very good at commanding and leading and controlling your own agency does not mean you'll be any good when everybody else shows up."[13]

Evidence suggests that this concern is justified. Even in less challenging circumstances, interagency coordination in Los Angeles has been problematic. During the Los Angeles riots of 1992, for example, the Los Angeles police chief requested National Guard support from the governor's office—which took three days to arrive—rather than calling the Los Angeles County sheriff's office for additional manpower, which could have arrived within one hour.[14] In 2002, a shooting inside Los Angeles International Airport (LAX) drew a relatively fast and overwhelming response (some 425 officers from 10 agencies arrived on the scene), but tensions between agencies ran high and it was unclear who had command of either crisis management or emergency response.[15] More recently, when a faulty transponder mistakenly signaled a hijacking of a Singapore Airlines flight in May 2004, federal officials failed to notify local authorities that it was only a false alarm. As a result, Los Angeles Airport Police stormed the plane with live ammunition when it landed. Once again, several agencies subsequently argued about who should have been in charge, with the Federal Bureau of Investigation (FBI) and the Los Angeles Police Department arguing that the Airport Police had violated protocols, but the Airport Police and Transportation Security Administration (TSA) insisting that appropriate action had been taken.[16] Reflecting on the confusion among the agencies sharing jurisdiction over security at the airport, one Los Angeles city council member commented, "Every addition to the alphabet soup

---

[13]Telephone interview with authors, 2005.

[14]Robert Garrot, Assistant Manager, Los Angeles County Emergency Operations Center, interview with Adam Clampitt, Monterey Park, California, February 4, 2003.

[15]Oldham (2002).

[16]According to Oldham, Krikorian, and Blankstein (2004), the TSA and Federal Aviation Administration (FAA) both knew of the transponder malfunction four hours before the Airport Police assaulted the plane, but no one shared this critical information with officials in Los Angeles. The TSA later argued that protocols did not require them to do so.

of agencies at the airport potentially adds to confusion in times of crisis."[17]

Following the September 11 attacks, the Coast Guard Captain of the Port began working with local, state, and federal agencies to develop a comprehensive security plan for the entire Los Angeles/Long Beach port complex. He assembled a Port Security Committee made up of eight county and municipal agencies, two state agencies, and four federal agencies, each with a different jurisdictional role. Chiefs and high-ranking command staff members represented the various agencies at quarterly meetings. A planning group began meeting three days per week to develop a "playbook" that cross-referenced attacks by type and location, outlined immediate steps for response, and noted primary points of contact for the various agencies.[18]

Findings and Recommendations

Although the establishment of the Port Security Committee was a step in the right direction, interviews with city and county agencies and political officials revealed significant information gaps in the planning process. Participation in the committee was voluntary and there was no formal protocol for keeping policymakers informed of progress. Most important, three sets of critical stakeholders were missing from the planning process: elected officials, public health officials, and private sector representatives.

Elected officials have a responsibility to ensure that broad goals are set for emergency response agencies, that priorities are made and sufficiently funded, that agencies talk to and work with one another, and that progress is evaluated. Elected officials also have the power to break bureaucratic logjams, particularly when responsibility for specific issues is unclear. Policymakers can meet these challenges, however, only when they collaborate across jurisdictional lines and actively engage in cooperative oversight.

---

[17]Oldham, Krikorian, and Blankstein (2004).

[18]George Cummings, Executive Officer, U.S. Coast Guard Marine Safety Office/ Group Los Angeles–Long Beach, interview with the authors, San Pedro, California, January 17, 2003.

We found, however, that elected officials from the relevant jurisdictions—the city of Los Angeles, the city of Long Beach, and Los Angeles County—were not equally informed about emergency response preparedness at the port complex and they were not collaborating actively to oversee the process. Instead, they had informally delegated this responsibility to local agencies and then relied on those agencies to keep them updated. This was problematic because agencies such as the Los Angeles and Long Beach Harbor Commissions functioned autonomously and governed the complex as two separate units. As a result, elected officials were not getting information about the entire port security picture. Indeed, in some cases, policymakers were not well informed about even their own piece of the port security picture. Some officials were unsure about which groups and organizations were involved in the planning process or they assumed that processes were actively working when in reality they had not yet begun.[19]

We found also that there was no medical or public health representative on the Port Security Committee. In the wake of the September 11 attacks and the subsequent anthrax scares, much national focus was placed on preparing for incidents involving weapons of mass destruction, especially bioterrorism and radiological "dirty bombs." Public health officials noted that the Los Angeles County Department of Health Services possesses a wealth of knowledge in these fields and public health involvement in emergency response planning at the port complex should be considered "a necessity."[20]

Finally, we found that private stakeholders were not included in the process. Specifically, associated organizations such as the International Longshore and Warehouse Union (ILWU) and the Pacific Maritime Association (PMA) had untapped expertise and material resources that could help response planning. The ILWU and other labor unions

---

[19]Confidential telephone interview with a senior law enforcement official, February 24, 2003; confidential telephone interview with a senior harbor commission official, March 19, 2003.

[20]Samuel Stratton, Medical Director, Los Angeles County Emergency Medical Services Agency, interview with Adam Clampitt, Los Angeles, California, February 11, 2003.

expressed dissatisfaction with the response planning process because they had not been invited to Port Security Committee meetings or asked to offer advice or resources. According to one union official, "ILWU hasn't been involved [by the Port Security Committee] yet and people on [the Marine Transportation System Safety and Security Subcommittee] don't listen."[21] Additionally, port workers told us that they felt that emergency response was being structured without their interests in mind. The same union official stated, "Employers are absolutely focused on commerce and couldn't care less about security."[22] The Pacific Maritime Association, which represents the shipping companies that use the port regularly and the terminal companies that carry out port operations, also expressed concerns about communication and involvement in the planning process.

We recognized that an optimal solution—such as realigning the two ports under a single political jurisdiction with one office responsible for emergency response planning and operations across both ports—was unfeasible. Seeking instead to maximize the effectiveness of the existing planning process, we recommended

- Creating a "Group of Five" to establish multijurisdictional political oversight for the port complex. This group would include the mayor of Los Angeles, the mayor of Long Beach, Los Angeles and Long Beach city council members whose respective districts include each port, and the Los Angeles County supervisor whose district includes the port complex. The Group of Five would meet with the Captain of the Port on a regular basis to set priorities, assess progress, and discuss concerns. In addition, it would work to secure funds for training exercises and equipment for the port complex.

---

[21]Luisa Gratz, President, International Longshore and Warehouse Union Local 26, interview with Adam Clampitt, San Pedro, California, February 25, 2003.

[22]Luisa Gratz, President, International Longshore and Warehouse Union Local 26, interview with Adam Clampitt, San Pedro, California, February 25, 2003.

- Adding a senior public health official to the Port Security Committee from the Los Angeles County Department of Health Services.
- Holding regular, periodic meetings between the Captain of the Port and/or the Port Security Committee and private sector stakeholders, such as industry and labor representatives.

Status of Implementation

To date, varying degrees of progress have been made toward implementing each of our recommendations. The Coast Guard was quick to make efforts to correct the inadvertent omission of public health agencies from the Port Security Committee's initial planning phases. During the course of our study, the Coast Guard contacted both the Los Angeles County Department of Health Services and the Centers for Disease Control and Prevention in an effort to incorporate them into the planning process at the port complex.[23] In addition, the Coast Guard Captain of the Port reiterated his commitment to encouraging all agencies with a role in the security of the port complex to participate in the Port Security Committee.[24]

Since the 2003 study was completed, the Coast Guard has also established a new organizational structure for coordinating port security planning. The Southern California Area Maritime Security (AMS) Committee was established pursuant to the Maritime Transportation Security Act.[25] The existing Port Security Committee formed the nucleus of the new body and other members were added to further improve port security planning and coordination. The implementing regulations specifically require the inclusion of maritime industry stakeholders, including labor, as well as port stakeholders "affected by

---

[23]Cummings (2003a).

[24]Cummings (2003b).

[25]Section 102 of the Maritime Transportation Security Act authorizes the Secretary of Homeland Security to "establish an Area Maritime Security Advisory Committee for any port area of the United States" and "request such a committee to review the proposed Area Maritime Transportation Security Plan . . . and make recommendations to the Secretary that the Committee considers appropriate."

security practices and policies."[26] As a result, representatives from the ILWU and other unions have been brought to the table, as have representatives of the PMA and individual ship operating companies. Thus, it has built on the success of the Port Security Committee and brought even more participants into the fold.

Although the AMS Committee is an excellent forum for information-sharing and planning coordination, it continues to suffer from three of the same problems as the Port Security Committee it superseded. First, the Coast Guard cannot compel membership in the AMS Committee; it can only invite participation. Second, the AMS Committee does not have any legal authority over participant (or non-participant) emergency response agencies or responders. If an agency does not like a policy decision that the AMS Committee makes, it is free to disregard it and walk away. Third, the AMS Committee does not have any budgetary authority over the participant emergency response agencies. It cannot force agencies to fund exercises and equipment purchases. In short, policy decisions made by the AMS Committee lack the legal authority to mandate action. Although successful in the short term, moreover, the committee has developed almost entirely through the personal efforts of Captain Neffenger and the informal relationships he has cultivated over several years with key stakeholders. Success over the long term requires greater institutionalization of the AMS Committee's membership, procedures, and norms and greater involvement of elected officials who have budgetary authority and political influence over the agencies involved in port security.

Bringing together the elected officials whose jurisdictions include the two ports proved to be more difficult than expected. After Los Angeles County Supervisor Don Knabe and former Los Angeles Mayor Richard Riordan became personally involved, key officials from the relevant jurisdictions finally agreed to meet. In September 2003, Supervisor Knabe, Los Angeles Mayor James Hahn, Los Angeles City Council Member Janice Hahn, Long Beach City Councilmember Dan Baker, and a representative from Long Beach Mayor Beverly O'Neill's office

---

[26] 33 C.F.R. Part 103.305(a).

gathered, along with officials from the Coast Guard, PMA, and ILWU, to discuss port security at the Los Angeles/Long Beach port complex.

Once these key players were in the same room, progress was made. According to Supervisor Knabe, "We have not had all these people sitting together at the table to discuss security needs at the ports of Los Angeles and Long Beach. . . . There may be two economic interests between the two ports, but there is one common concern about security and we should address it together."[27] The meeting accomplished three key goals: The Group of Five agreed that port workers should receive Community Emergency Response Team (CERT) training (discussed further below), and Mayor Hahn tasked the Los Angeles Fire Department to train them; all parties agreed that the two cities must coordinate their efforts to apply for federal port security funds; and local news media covered the event, which both acted as positive reinforcement for the officials and raised greater awareness of the issues with the public.

Continued cooperation and focus are required to ensure ongoing progress. Although the five elected officials with political responsibility for the port complex regularly send staff to AMS meetings, the principals have met with the Coast Guard Captain of the Port only once since September 2003, at a port security briefing and press conference that Senator Dianne Feinstein organized in February 2005. The multijurisdictional nature of the port complex and the lack of a single governing body with authority over all of the entities involved necessitate that elected officials play an integral role in overseeing the coordination of port security and emergency response.

We believe that the Group of Five meeting is essential for at least four reasons. First, port security is a multijurisdictional policy issue that requires senior-level focus to stimulate action. Second, relying on staff to manage this effort risks everyday pitfalls, including both poor communication and internal politicking. Third, the meeting facilitates implementation throughout the bureaucracy because it symbolically institutionalizes support for the Coast Guard as the de facto lead agency in the port security effort. Fourth, it helps compensate for the fact that

---

[27]Office of Los Angeles County Supervisor Don Knabe (2003).

the media and the public pay less attention to port security than they should. In these ways, the meetings serve as action-forcing devices for the Coast Guard to identify key issues where it needs help, for different agencies to make progress, and for political officials to get up to speed. Given these benefits, we believe that the political principals should continue to send their staff to AMS meetings, but that the Coast Guard should also host a semi-annual summit for the Group of Five. Supervisor Knabe and Captain Neffenger have stated their desire to host another summit in the near future.

Conceptual Challenges

Background

Developing effective governance for emergency response at U.S. ports requires more than good organizational arrangements. It requires conceptual innovation, determining the extent to which old models apply, and then adapting past practices to meet new challenges. We found that California's extensive experience in handling natural disasters spelled both good and bad news for thinking through port security issues. On the one hand, Southern California's emergency response agencies were more accustomed to interagency collaboration than most of their counterparts in the United States. Years of experience, however, had also led decisionmakers to assume that traditional models of emergency response were well suited to handling a terrorist incident at the Los Angeles/Long Beach port complex—an assumption we found to be questionable.

Traditional emergency response plans call for dispersing personnel and equipment across a community—to provide broad coverage for routine emergencies—and moving those resources to disaster areas when necessary. Predictably, emergency response agencies such as firefighters and police have a very small contingent on duty at the port complex at any given time. Between the Los Angeles Port Police, Port of Long Beach Harbor Patrol, Los Angeles Fire Department, Long Beach Fire Department, and Coast Guard, only about 100 sworn law enforcement officers and firefighters are directly assigned to the port complex and on

duty during a typical shift.[28] Any significant incident would require assistance from other public safety agencies throughout Los Angeles County, including the Los Angeles Police Department, Long Beach Police Department, Los Angeles Sheriff's Department, and FBI. This is understandable. These agencies have extensive personnel and materiel resources, but they also have broad geographical areas of responsibility. Despite the economic importance of the port complex, these agencies cannot deploy their resources in a way that favors the complex at the expense of other areas in their jurisdictions except in the event of a crisis.

The traditional surge model for emergency response makes sense in general—first responders cannot be everywhere all of the time. The problem is that for surge capacity to work well, it must work fast. This is not likely to be the case at the Los Angeles/Long Beach port complex under ordinary circumstances and is even less likely in the event of a terrorist attack.

Because of the harbor's location, many emergency response personnel will need to drive to the port complex from other locations throughout Los Angeles County. But as shown in the port map on p. xxiii, access to many areas of the port complex is quite limited, with the Harbor Freeway (110) and Long Beach Freeway (710) the primary roadways into the port area. An estimated 35,000 cargo truck trips are made to and from the port complex using these freeways each day.[29] This means, for example, that any first responders traveling in traffic from downtown Los Angeles—where the Los Angeles Fire and Police Departments are headquartered—would take between one and one and a half hours to arrive.[30] Indeed, a Los Angeles Fire Department battalion chief who works within the port complex expressed concern that first responders may experience significant delays while trying to get to the port after a terrorist attack.[31] In addition to normal lags in response

---

[28]This information is based on interviews with the various law enforcement and fire agencies at the port complex from January to March 2003.

[29]Fox (2004).

[30]Wachs (2003).

[31]Louis Rupoli, Battalion Chief, Los Angeles Fire Department, interview with Seth Jacobson, San Pedro, California, January 10, 2003.

times, a traffic accident or an incident that occurred during rush-hour would likely leave the port complex without substantial outside assistance for several hours. Analysts have called the 710 "the most accident prone freeway in Southern California."[32] The concentration of port-related traffic, moreover, increases the likelihood that such accidents would involve large trucks, which take longer to clear. Although systematic data are unavailable, recent examples provide some evidence that the potential delays are substantial. In September 2003, the crash of a gasoline tanker truck closed the freeway for more than 12 hours.[33] In October 2003, another truck crash closed the freeway for eight hours.[34]

In a terrorist attack, moreover, the potential for mass panic and the need to evacuate communities pose additional risks of gridlock on major roadways approaching the port complex. In one recent survey, 40 percent of respondents said they would ignore instructions from public officials to stay where they are after a radiological attack, with most choosing instead to return home, causing further delays on the roads.[35] Evacuations in the Los Angeles/Long Beach area, moreover, are conducted by different agencies in different political jurisdictions, raising the very real possibility that insufficient coordination across individual evacuation efforts could make matters worse, clogging roadways, increasing panic, and preventing first responders from reaching the port.

These realities suggest the need for thinking differently about emergency response to a terrorist attack at the port complex: Citizens should be treated not merely as potential victims but also as crucial first responders. Although the term first responder typically refers to firefighters and other emergency services agencies, the reality is that citizens usually function as the true first responders when tragedy strikes. Disasters such as the Mexico City earthquake of 1985 and the September 11 attacks on New York City and Washington have shown that family members, coworkers, and neighbors are often first on the scene. Untrained civilians saved more than 800 people after the Mexico City

---

[32] Jergler (2003).

[33] Bernstein and Schoch (2003).

[34] Bernstein, Hoffman, and Schoch (2003).

[35] Lasker (2004), pp. 8, 32.

earthquake, but at least 100 civilians died while trying to save others.[36] Israel has trained approximately 100,000 civilians to aid in response to terrorist events. As these examples indicate, emergency response planning can make use of the natural inclinations of citizens to help by training populations in vulnerable areas how to help themselves and others until professional emergency response personnel can arrive. Well-managed civilian teams can work as force multipliers and expand emergency response capabilities.[37]

Although Los Angeles has led the country in developing such civilian training programs, these programs have been underfunded, underutilized, and unfocused. The result has been that opportunities to dramatically enhance emergency preparedness at the port complex have not been realized.

Community Emergency Response Teams

In 1985, the Los Angeles Fire Department developed a program for training civilians called Community Emergency Response Team. The original 17-hour training program was created to train civilians to provide assistance "during disaster situations where the number and scope of incidents have overwhelmed the conventional emergency services."[38] The course was designed primarily for groups such as community organizations and businesses. Graduates of the course are prepared to function both as members of a CERT team and as individual leaders who would direct untrained volunteers during the initial phases of an emergency.[39]

The Federal Emergency Management Agency (FEMA) adopted the Los Angeles Fire Department's CERT model and since the September 11 attacks has been directing grants to fund civilian CERT programs in all

---

[36]According to http://training.fema.gov/emiweb/CERT/overview.asp, accessed July 1, 2005.

[37]Jim Harkins, Firefighter, Los Angeles Fire Department Disaster Preparedness Unit, interview with Seth Jacobson, Los Angeles, California, January 22, 2003.

[38]Los Angeles Fire Department (n.d.).

[39]Los Angeles Fire Department (n.d.).

50 states.[40] FEMA seeks to double the number of CERT-trained civilians to 400,000 by 2005.[41] Although funds are limited, local officials have discretion over where their CERT allocations are spent and who receives priority in training programs.

Findings and Recommendations

Given the size of the port complex, its limited access, and its potential vulnerability to terrorist attack, the study found general agreement that workers at the port complex should receive CERT training. The ILWU, other harbor-based unions, and the PMA agreed,[42] as did the management at the four local emergency response departments, who believed that providing CERT training to port workers would generate substantial additional support for their emergency response plans.

Despite general agreement that training was needed, the study identified four overarching impediments to the effective training of port workers. First, there were no established priorities for allocating the scarce CERT training resources throughout Los Angeles County and its municipalities. Second, there were not enough CERT instructors available to participate full-time in an effort to train the port workers. Third, there were not enough local funds available to pay for a concerted CERT training effort at the port complex. Fourth, civilian volunteers did not have ready access to first aid or rescue equipment at the port complex.

As a result of the near-universal agreement between first responders, industry, labor, and policymakers, the study recommended that the Los Angeles County CERT Advisory Committee—the interagency group that oversees CERT allocations in the county—make a dedicated effort to train workers at the port complex. Specifically, we recommended:

---

[40]Federal Emergency Management Agency (2005).

[41]Citizen Corps (2005).

[42]Luisa Gratz, President, International Longshore and Warehouse Union Local 26, interview with Adam Clampitt, San Pedro, California, February 25, 2003; Bob Dodge, Vice President of Training, Pacific Maritime Association, interview with the authors, Long Beach, California, March 5, 2003.

- **CERT training:** The CERT Advisory Committee should prioritize high-risk populations, allocate CERT classes first to these high-priority groups, and set target percentages of volunteers to be trained within these populations. Port workers should then receive CERT training because the port complex is a high-risk target for terrorism.
- **Interagency Joint Training Team:** To overcome resource constraints, the CERT Advisory Committee should coordinate the creation of an Interagency CERT Joint Training Team for the port complex. The Los Angeles and Long Beach Fire Departments, Los Angeles County Fire Department, and Los Angeles Sheriff's Department should each dedicate one full-time CERT trainer from their existing staffs to train workers at the port complex. In addition, the American Red Cross should teach CERT modules that do not require instruction by professional first responders.
- **CERT funding:** The CERT Advisory Committee should pursue both federal grants and private sector donations as funding alternatives for the interagency CERT Joint Training Team.
- **CERT materiel:** The interagency CERT Joint Training Team should provide each CERT-trained port worker with a small equipment kit. Many first response officials and port workers agreed that instead of using stockpiled caches of equipment, CERT-trained port workers should be allocated individual kits of first aid and safety equipment to keep with them at their job sites.

Status of Implementation

Initially, despite consensus about the need and value of CERT training, no action was taken because the program, like port security issues more broadly, fell across multiple political jurisdictions. We then took two steps to move the process forward. First, we made CERT training the focus of the first Group of Five meeting. The idea was to focus political attention on a concrete issue that already had the backing

of key constituency groups to propel it forward. Both labor and management representatives attended the meeting and signaled their agreement on the outlines of a CERT program. Second, we designated one member of our team to be the point person for monitoring progress and coordinating implementation of the program on the ground.

The strategy proved successful at breaking the impasse. At the Group of Five meeting in September 2003, all local officials agreed that the port workers must receive CERT training to prepare them to respond to an attack. Mayor Hahn then tasked the Los Angeles Fire Department with meeting this goal and with giving port workers highest priority in the program. Thanks to the mayor's leadership, the Fire Department has now allocated priority to port workers and training has begun.

As of February 2006, 250 ILWU warehouse guards have undergone an abridged eight-hour CERT program that fulfilled a contractual agreement for training between the labor union and management and 55 port workers have received the full 20-hour CERT course.[43] The Coast Guard, the Los Angeles Fire Department, and the ILWU are tailoring the CERT curriculum specifically to address hazards at the port complex. Moreover, the Coast Guard is developing plans to include CERT-trained workers in its emergency response exercises.

After the release of our report, the Los Angeles County Sheriff's Department, the Los Angeles County Fire Department, and the American Red Cross began to coordinate efforts to provide CERT training to citizens throughout Los Angeles County. However, an Interagency Joint Training Team for the port complex has not been established. Instead, the Los Angeles Fire Department is planning to provide the CERT training at the port complex.

Given the lack of a joint training team for the port complex, the CERT Advisory Committee has not pursued federal grants and private sector donations as funding alternatives for a CERT training program for port workers. The Area Maritime Security Committee's Subcommittee on Training and Exercises, however, is exploring these funding alternatives to support the CERT program at the port complex.

---

[43]Gerlich (2004).

Small equipment kits have not yet been provided to trained workers. The Area Maritime Security Subcommittee on Training and Exercises has begun to discuss how to obtain these kits from either the American Red Cross or the private sector.

Much remains to be done. Specifically, the CERT program needs to

- **Establish and meet training targets:** With projections of 20,000 unionized maritime workers at the port complex by 2006, it may take years to train a few thousand of them. The CERT training program must set aggressive but reasonable targets for the number of workers to be trained and must meet these training goals.
- **Augment CERT training resources:** The Los Angeles Fire Department's Disaster Preparedness Unit staffs only six full-time CERT trainers for the city of Los Angeles. It may lose additional trainers to injuries, budget cuts, or National Guard call-ups. Satisfying training demands at the port complex will likely require working with statewide officials to garner greater resources from Washington, D.C., involving the private sector, creatively managing existing countywide CERT resources, or some combination thereof. The Los Angeles County Sheriff has indicated support for solving this resource gap with a Joint Training Team.[44]
- **Integrate trained workers into exercises:** The workforce has not participated in homeland security drills at the port complex. Coast Guard and other planning agencies must include at least those workers who have received CERT training.
- **Review, revise, and improve:** The plan must include a feedback process for evaluating the effectiveness of the training and for improving on this program where possible.

---

[44]Leroy Baca, Sheriff, Los Angeles Sheriff's Department, phone interview with Seth Jacobson, May 24, 2005.

Obstacles and Success Factors

Taking a step back, we find three major obstacles to the fast and effective improvement of governance capabilities for emergency response at the port complex. The first has to do with the nature of the problem. Homeland security policy in general—and port security emergency response in particular—is a thorny, complex, and new issue for local officials. There is no standard literature on port security emergency response, no clearly established set of best practices. Although aspects of emergency response are old, key elements related to counterterrorism are new and changing constantly. As a result, developing expertise takes time and sustained attention, the two resources in shortest supply for most local elected leaders, their staffs, and agency officials. Our original study of the ports of Los Angeles and Long Beach took more than eight months of full-time work by a team of five, and implementation of our recommendations—which we thought could be done in three to six months—is still in progress three years later.

The second constraint is related to the first: Political incentives to take action in port security are weak. From a politician's point of view, port security emergency response planning is the worst of all worlds: It requires extremely high up-front costs for benefits that will be realized only in the future—most likely when the official is already out of office—or perhaps never. In addition, making homeland security policy requires making tough choices about where to dedicate limited resources. These are exactly the kinds of choices many politicians try to avoid. When such choices cannot be avoided, longer-term planning usually takes a back seat to shorter-term gains. Consider, for example, a mayor who must decide whether to dedicate additional police officers to lowering the crime rate or enhancing counterterrorism surveillance at the port. Any politician with a reasonably developed sense of self-preservation focuses on crime and leaves port security for another day.

Moreover, even within the area of homeland security, electoral incentives create sub-optimal policy outcomes. The natural impulse of any elected official is to focus on issues of greatest concern to constituents. This sounds good in theory. The problem is that it works poorly in practice. Most California citizens are concerned about

terrorism, but few have visited the port complex or worry about its security, and fewer still pay close attention to the details of how elected officials handle the arcane details of CERT training or cross-agency coordination. Instead, since the September 11 attacks, the public and the press have focused their concern on higher-visibility targets such as LAX and the security of local drinking water supplies.

The misplaced allocation of homeland security dollars can be seen at every level of government. In December 2004, former DHS Inspector General Clark Kent Ervin articulated this in a report titled "Major Management Challenges Facing the Department of Homeland Security."[45] Since September 2001, Congress has distributed more than $13 billion to state governments with a formula only Washington could concoct: 40 percent was split evenly, regardless of a state's population, targets, or vulnerability to terrorist attack. Although rural states with fewer potential targets and low populations, such as Alaska and Wyoming, received more than $55 per resident, target-rich and densely populated states, such as New York and California, were short-changed. New York received $25 per person, California just $14. California's state officials used a similar formula to distribute federal funds within the state, exacerbating the underfunding of urban areas.[46] This misallocation may be starting to change with the decision in early 2006 by DHS to distribute fiscal year 2006 federal Urban Areas Security Initiative grants on the basis of risk rather than a strict formula.

At the local level, Los Angeles's most publicized initiative has been a controversial $11 billion plan to expand and relocate portions of Los Angeles International Airport.[47] To put the plan's price tag into some perspective, it would cost nearly 20 times more than the federal

---

[45]U.S. Department of Homeland Security (2004).

[46]California allocates federal funds from the State Homeland Security Program (SHSP) using a "base plus population" formula. According to California Office of Homeland Security (2005), the state distributed approximately $67.7 million as part of the fiscal year 2005 SHSP grant program. Each county was awarded a base amount of $100,000 and the remainder was allocated on the basis of each county's population. As a result, Alpine County (population 1,280) was awarded $102,192, or $79.84 per capita. Los Angeles County (population 10.1 million) was awarded $17.4 million, or $1.72 per capita.

[47]For a useful analysis of the plan, see Schell, Chow, and Grammich (2003).

government's grants for port security since September 11. In short, political incentives create strong pressures for local elected officials to put the right emphasis on the wrong issues.

Third and finally, the multijurisdictional boundaries of the port complex pose significant problems. Who exactly is responsible for overseeing the planning and operation of emergency response at the ports of Los Angeles and Long Beach? The answer is everyone and no one. Although the Coast Guard Captain of the Port has made great strides in serving as the de facto coordinator of all city, county, state, and federal agencies involved in port security, he holds no control over key assets, he serves a mission that encompasses far more than local emergency response, he does not have a permanent post, and he cannot succeed without help. Bureaucratic rivalries between the two ports, the two cities, and the layers of governmental agencies make that help difficult to get.

The CERT training initiative described above highlights the difficulties created by the port complex's fragmented political authority. Even this program, which was funded by the federal government and which was supported by every major stakeholder at the port, including both labor and management, did not initially succeed; no one office and no one official had responsibility for making it happen. Only when Mayor Hahn took the initiative to create that responsibility by designating the Los Angeles Fire Department as the main agency point of contact did training begin. His successor, Mayor Antonio Villaraigosa, must build on the current commitment to implementing this effort.

Key Success Factors

Despite these obstacles, progress has been made. Looking back, we find three key factors for success: neutral analysis, long-term involvement, and political leadership.

- **Neutral analysis:** As outsiders, we had certain advantages and disadvantages while working to implement the recommendations from the 2003 study. The majority of these factors seemed to work in our favor. For example, as a third party, we were able to operate as a neutral broker—especially

between organizations that have traditionally been somewhat adversarial, such as the labor unions and the shipping association. Because we were not already entrenched in a position, many agencies and organizations were willing to speak more frankly with us than other agencies that were more involved. In addition, because we were a new set of eyes looking at the issues, we were often able to provide a different perspective, or at least a perspective that looked across agency boundaries. Although individuals and agencies had critical pieces of the puzzle, no one agency or person had ever put those pieces together.

- **Long-term involvement:** Policy analyses often identify problems and recommend solutions but then move on to new issues. We started with such an approach but soon realized that success required a long-term commitment. Neutrality provides credibility, but not trust. Particularly in an area where the best data sources are people, building relationships with stakeholders was crucial for determining weaknesses and developing strategies to overcome them. This has meant spending a significant amount of time being physically present at the port complex, meeting and talking with people. Although much remains to be done, it is clear from this experience that achieving any serious progress requires that policy analysts become policy partners.
- **Political leadership:** There is no substitute for the power of personal political leadership. This maxim is particularly true when formal political power is fragmented or unclear. Our outsider status was a clear disadvantage for policy implementation in this environment; we had neither the power nor the influence to begin to implement our recommendations throughout the fragmented port jurisdictions. Supervisor Knabe's personal contact with each of the key policymakers was therefore instrumental in overcoming resistance to holding the Group of Five meeting. Moreover, Mayor Hahn cut through the multijurisdictional confusion about who should provide CERT training for the port workers by tasking the Los Angeles

City Fire Department with getting the job done. Similarly, Coast Guard Captain Peter Neffenger and his predecessor Captain John Holmes used personal political leadership more than statutory authority to create new coordinating committees to share information, oversee planning, and facilitate cooperation across agencies, companies, and other stakeholders. Not surprisingly, we found that officials, when they choose, can play a fundamental role in setting priorities, shaping perceptions, and overcoming resistance.

Conclusion

Several years after September 11, California's seaports remain highly vulnerable to terrorist attack. A recent report by the Government Accountability Office identified ongoing weaknesses in the federal programs to secure roughly 8.4 million containers entering the United States each year.[48] As one Coast Guard official at the ports of Los Angeles and Long Beach put it, "Once a ship enters the harbor, we're in response mode, not prevention."

Developing effective governance for America's seaports is not easy. The port complex at Los Angeles and Long Beach presents one target, but its safety depends on 15 agencies, two cities, two mayors, five county supervisors, 10 harbor commissioners, and 24 city council members operating under a number of federal, state, and local guidelines that assign management for emergency response to different agencies depending on the circumstances. Who is in charge? The answer is "it depends." The organizational challenges created by these legal and political realities are, not surprisingly, large. Although progress has been made with the Area Maritime Security Committee and the Group of Five, much more remains to be done to foster collaboration between government agencies, private sector stakeholders, and the public.

But organizational fixes are not enough. Improving governance requires more than making the machinery of government run better. It requires infusing the governance process with new ideas and analysis to ensure that the assumptions of the past do not prevent an effective

---

[48]U.S. Government Accountability Office (2005).

response in the future. This case study suggests that a useful place to start is by redefining who first responders are—training civilians to assist their own communities, particularly in locations that are considered major terrorist targets and are relatively inaccessible to emergency response agencies.

Making these improvements will take time, and, more importantly, sustained attention and leadership by local political officials.

Interviews

For the 2003 study, we and our coauthors conducted interviews with numerous agencies, policymakers, labor and industry representatives, and emergency service workers at the local, state, and federal levels. This report drew on much of that research for background information. In addition, while preparing this report, we conducted follow-up interviews with many of the same agencies, groups, and individuals.

Alameda Corridor Transit Authority
American Red Cross
Bassett Sales Corporation
California Governor's Office on Service and Volunteerism
California Homeland Security Advisory Council
California Office of Emergency Management
California State Office of Emergency Services, Coastal Region
Capitol Corridor Joint Powers Authority
Disaster Consultants Inc.
Emergency Network of Los Angeles
Federal Bureau of Investigation
Governor Michael S. Dukakis
Harbor-UCLA Medical Center
Houston Port Authority
International Longshore and Warehouse Union
International Organization of Masters, Mates and Pilots
Long Beach Fire Department
Long Beach Harbor Commission
Long Beach Police Department
Los Angeles City Emergency Preparedness Department

Los Angeles City Fire Department
Los Angeles County Board of Supervisors
Los Angeles County Emergency Medical Services Agency
Los Angeles County Office of Emergency Management
Los Angeles Police Department
Los Angeles Port Police
Los Angeles Sheriff's Department
Marine Firemen's Union
Marine Transportation System Advisory Council
Mayor Richard Riordan
Miami Dade Metropolitan Police Department
Miami Seaport
Office of Los Angeles City Councilman Jack Weiss
Office of Los Angeles City Councilwoman Janice Hahn
Office of Long Beach Mayor Beverly O'Neill
Office of United States Congresswoman Jane Harman
Pacific Maritime Association
Sailors Union of the Pacific
Science Applications International Corporation (SAIC)
Transportation Security Administration
United States Coast Guard
University of California, Berkeley, Department of City and Regional Planning
University of California, Los Angeles, Department of Urban Planning
University of California, Los Angeles, School of Public Health
University of California Police Department
U.S. Department of Transportation
Verizon Communications Corporation

References

Allen, Warren T. II, Adam Clampitt, Matthew Hipp, and Seth Jacobson, *Port Security Applied Policy Project: Recommendations to Improve Emergency Response Capabilities at the Port of Los Angeles and the Port of Long Beach,* University of California, Los Angeles, California, May 16, 2003, available at www.riuhs.org/publications/documents/PortSecurity.pdf (as of April 30, 2006).

Bernstein, Sharon, and Deborah Schoch, "Tanker Truck Blast Kills Driver, Forces Evacuations," *Los Angeles Times,* September 24, 2003, p. B3.
Bernstein, Sharon, Allison Hoffman, and Deborah Schoch, "6 Killed When Big Rig Loses Control on 710," *Los Angeles Times,* October 10, 2003, p. B1.
California Office of Emergency Services, *State of California Emergency Plan,* Sacramento, California, 1998.
California Office of Homeland Security, Governor's Office of Emergency Services, *FY05 Homeland Security Grant Program: California Supplement to the Federal Program Guidelines and Application Kit,* Sacramento, California, 2005.
Citizen Corps, "Programs and Partners: Community Emergency Response Teams (CERT)," available at www.citizencorps.gov/programs/cert.shtm (as of July 1, 2005).
Code of Federal Regulations, Title 33, Part 103, Area Maritime Security.
Cummings, George, email to Matthew Hipp, February 24, 2003a.
Cummings, George, email to Matthew Hipp, March 11, 2003b.
Drabek, Thomas E., and Gerard J. Hoetmer, *Emergency Management: Principles and Practice for Local Government,* International City Management Association, Washington, D.C., 1991.
Federal Emergency Management Agency, Emergency Management Institute, "Community Emergency Response Team Overview," available at training.fema.gov/emiweb/CERT/overview.asp (as of July 1, 2005).
Fox, Sue, "Plan Aims to Reduce Truck Congestion at Ports," *Los Angeles Times,* August 22, 2004, p. B6.
Gerlich, Stacy, Firefighter, Los Angeles Fire Department Disaster Preparedness Unit, email to Seth Jacobson, October 27, 2004.
Homeland Security Presidential Directive/HSPD-5, "Management of Domestic Incidents," *Weekly Compilation of Presidential Documents,* Vol. 39, Washington, D.C., March 10, 2003.
Hymon, Steve, "LAX Ranks No. 1 on List of State Terrorist Targets," *Los Angeles Times,* February 22, 2003, p. B1.
Jergler, Don, "Freeway Change Debated," *Long Beach Press-Telegram,* April 3, 2003.

Lasker, Roz, *Redefining Readiness: Terrorism Planning Through the Eyes of the Public,* September 14, 2004, available at www.cacsh.org/pdf/RedefiningReadinessStudy.pdf (as of January 28, 2005).
Los Angeles Fire Department, "Community Emergency Response Team Program: Course Syllabus," available at www.cert-la.com/CERT-Syllabus.pdf (as of July 1, 2005).
Maritime Transportation Security Act of 2002, Public Law 107-295, Washington, D.C., November 25, 2002.
Neffenger, Peter, Coast Guard Captain of the Port, Port of Los Angeles/Port of Long Beach, "U.S. Coast Guard Sector Los Angeles–Long Beach," presentation at the School of Public Affairs, University of California, Los Angeles, California, November 2, 2005.
Office of Los Angeles County Supervisor Don Knabe, *Knabe Hosts Port Security Summit of Leading Local Officials,* Los Angeles, California, September 25, 2003.
Oldham, Jennifer, "Response to LAX Shooting Flawed, Study Says," *Los Angeles Times,* October 7, 2002, p. B3.
Oldham, Jennifer, Greg Krikorian, and Andrew Blankstein, "Agencies Criticize LAX Handling of Hijack Alert," *Los Angeles Times,* May 6, 2004, p. B1.
Schell, Terry L., Brian G. Chow, and Clifford A. Grammich, *Designing Airports for Security: An Analysis of Proposed Changes at LAX,* the RAND Corporation, IP-251, Santa Monica, California, 2003.
Stumpf, Jim, "Incident Command System: The History and Need," *The Internet Journal of Rescue and Disaster Medicine,* Vol. 2, No. 1, 2001, available at www.ispub.com/ostia/index.php?xmlFilePath=journals/ijrdm/vol2n1/ics.xml (as of July 1, 2005).
U.S. Department of Homeland Security, "Major Management Challenges Facing the Department of Homeland Security," December 2004, available at http://www.dhs.gov/interweb/assetlibrary/OIG_05-06_Dec04.pdf (as of January 28, 2005).
U.S. Government Accountability Office, *Homeland Security: Key Cargo Security Programs Can Be Improved,* GAO-05-466T, Washington, D.C., 2005.
Wachs, Martin, Director, Institute of Transportation Studies, University of California, Berkeley, email to Seth Jacobson, March 4, 2003.

7. The Government Response: U.S. Port Security Programs

Jon D. Haveman and Howard J. Shatz
Public Policy Institute of California

Ernesto Vilchis
Princeton University

> The Department of Homeland Security envisions a system for supply chain security that mitigates the evolving terrorist threat and facilitates the free flow of global commerce in order to ensure the physical and economic well being of the United States and its trading partners. In enacting this vision, DHS seeks to bring to bear the collective resources and efforts of all stakeholders, while enhancing the integrity of the supply chain.
>
> *Vision statement for cargo security.*[1]

Introduction

In their effort to deliver port and maritime security, U.S. policymakers faced a daunting set of programmatic challenges following the September 11, 2001, terrorist attacks. They had to first determine the tradeoffs between maritime security and other homeland security concerns, and to then decide where the greatest maritime threats and vulnerabilities lay, identify which types of threats might cause the most harm to the United States, and then choose how best to enlist the diverse and sometimes combative members of the maritime community in a united security effort. Most of all, they had to decide how to balance these security efforts with what they were trying to protect: the benefits from international trade and an open trading system. As Flynn (2002) notes, "Ultimately, getting homeland security right is not about constructing barricades to fend off terrorists. It is, or should be, about

[1]U.S. Department of Homeland Security (2004b).

identifying and taking the steps necessary to allow the United States to remain an open, prosperous, free, and globally engaged society."

Policymakers have authorized port security measures that fall into five related classes: planning for protection, response, and recovery; hardening ports to make them less-attractive targets; sealing gaps in international supply chains—the points where terrorists, their supplies, or their weapons could enter shipping channels; identifying and closing security weaknesses outside the United States, preferably in foreign countries before the goods start their journey here; and upgrading technologies to accomplish the first four tasks.

The Maritime Transportation Security Act of 2002 (MTSA), supplemented by the Coast Guard and Maritime Transportation Act of 2004, dominates the effort to secure the maritime supply chain.[2] MTSA sets out broad guidelines for securing the nation's ports and related intermodal facilities. Tasked with implementing many of the MTSA measures, the U.S. Coast Guard has become the lead agency in maritime and port security. The Coast Guard is also responsible for overseeing for the United States the implementation of the International Ship and Port Facility Security (ISPS) Code, measures that broaden maritime security planning and preparedness to the whole world and that were developed by the International Maritime Organization (IMO).

A second federal agency, U.S. Customs and Border Protection, has launched two programs aimed at sealing weak points in global supply chains and moving security efforts beyond the U.S. border. These are the Customs Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI). The C-TPAT encourages shippers and carriers to implement security plans and measures to promote greater security at all points along the supply chain. The CSI facilitates the inspection of high-risk containers for hazardous materials at the foreign port of origin, long before the containers reach U.S. shores. Other programs, including port security grants, are also part of the mix and are administered by different agencies, such as the Transportation Security

---

[2] MTSA is U.S. Public Law 107-295, and the Coast Guard and Maritime Transportation Act of 2004 is U.S. Public Law 108-293.

Administration, the U.S. Maritime Administration, and the U.S. Department of Homeland Security's Office of Grants and Training.

It is extremely difficult to evaluate whether these programs have made the country safer without detailed on-site investigation and without full disclosure by federal agencies. This uncertainty extends throughout the federal government itself. At a Congressional hearing in 2005 about a major U.S. Coast Guard acquisition program known as the Integrated Deepwater System, Representative Marion Berry of the District of Columbia told the Commandant of the Coast Guard, Admiral Thomas H. Collins, "Admiral, with all due respect to you gentlemen, I sincerely hope that you know more about what you're doing than I think you do. I have never seen such a conglomeration of mumbo jumbo in all my days, and you scare me to death."[3] Hearings, government reports, and informal conversations with officials throughout the maritime world indicate that progress is being made, but the challenges are extremely complex and the adversary is adaptable. It may be impossible ever to gauge how well protected the nation is.

This chapter paints the landscape of current U.S. port security programs, discussing efforts both to protect ports and to prevent international goods movement from being used as a vector for terrorists, their weapons, or their supplies. The next section introduces U.S. government thinking in the years leading up to the September 11 attacks, and the following section gives more details about each of the main port security efforts. The section after that evaluates these efforts and indicates how well they protect ports in the state of California. California serves as a valuable case because it hosts three of the 10 largest U.S. seaports by value—Los Angeles, Long Beach, and Oakland—and because the combined port complex of Los Angeles and Long Beach constitutes the fifth-largest container port in the world in terms of container volumes. The final section draws conclusions.

Port Security Before the September 11 Attacks

Before the terrorist attacks on New York and Washington in 2001, port security focused on physical security and access control, cargo

[3]Federal News Service (2005b).

security, passenger and crew security, and military mobilization security and was oriented toward crime-related activities. Although the maritime community acknowledged the threat of terrorism, very few specific security measures were taken to deter or undermine a maritime terrorist threat. Indeed, some simple measures, such as requiring identification to enter sensitive areas, were largely absent in many U.S. ports. Despite this neglect, the U.S. government in the late 1990s had initiated several efforts regarding protection of the ports.

In 1997, the Department of Transportation (DOT) released *Port Security: A National Planning Guide.*[4] This report provided an overview of security issues and other challenges facing U.S. ports and discussed many of the essential ideas that were to become the core of the current U.S. strategy on port security. For example, the guide highlighted the need for port authorities to develop and implement port security plans. It also raised issues about how available technologies would be exploited and how new ones would be developed, as well as the need for greater international cooperation. Meant to be the first in a series, the report was to be followed by technical manuals for planning and conducting daily operations of port security. Despite the importance of the topics covered, the report did not discuss any requirements for implementing new port security measures. Rather, it claimed that implementation of these measures by ports would be good business, with savings more than offsetting expenditure.

Another pre-September 11 effort was the Marine Transportation System (MTS) Initiative, begun in 1998, and which incorporated the work of a large number of agencies connected with ports and the U.S. waterway system, including the Coast Guard, the U.S. Maritime Administration (MARAD), the U.S. Army Corps of Engineers, the National Oceanic and Atmospheric Administration (NOAA), and the Environmental Protection Agency (EPA). The original impetus for the MTS was a realization that the system's infrastructure, particularly inland locks and dams, was aging and perceived to be inadequate to handle the expected growth in maritime activities. Although port security was not the exclusive focus of the MTS Initiative, it was a core element.

---

[4]U.S. Department of Transportation (1997).

The MTS Initiative identified a set of barriers to effective response to the threat of terrorism and suggested solutions to overcome these barriers. Key barriers included insufficient national awareness of the MTS as a critical element of U.S. infrastructure, lack of integrated federal leadership on security issues, insufficient resources to address security gaps, and lack of established minimum security standards and operating guidelines. The security panel at an MTS-Initiative-related national conference in November 1998 issued a set of policy recommendations designed to address these factors, including developing security standards, staging terrorism exercises, designating a lead agency for MTS security, and developing systems for tracking cargo, personnel, and vessels.[5]

Late in 1998, Congress directed the creation of an MTS Task Force to "assess the adequacy of the Nation's marine transportation system . . . to operate in a safe, efficient, secure, and environmentally sound manner."[6] The Task Force's report, issued September 1999, recognized that rogue states and transnational terrorists could target U.S. critical infrastructure, including seaports. Passenger ships were singled out as a particularly potent terrorist opportunity. Critical issues included the lack of national security awareness of the MTS, the lack of federal leadership on the issue, and the inability to track cargo, people, and vessels through the system. Recommendations included developing national exercises, instituting tracking systems, forging public-private partnerships within the United States, advancing U.S. standards internationally, and providing international intelligence and training. The report also discussed incorporating preexisting local Harbor Safety Committees into the MTS goals of safety and environmental protection. Their role has since been extended to include security.[7]

Reinforcing the efforts of Congress, President Bill Clinton in April 1999 established a commission to undertake a comprehensive study of crime in U.S. seaports and to examine the potential threats posed by terrorists and others to the people and critical infrastructures of seaport

---

[5]U.S. Department of Transportation (1998).

[6]Marine Transportation System Task Force (1999).

[7]Loy (2002).

cities. Aside from its own investigations, this commission received recommendations from the MTS Task Force. The result, in 2000, was the publication of the *Report of the Interagency Commission on Crime and Security in U.S. Seaports*. At the time the report was published, the FBI considered the threat of terrorism directed at U.S. seaports to be low but also considered their vulnerability to be high, and the commission expressed the belief that an attack had the potential to cause significant damage.

The report indicated the need to consider seaports as a part of an "intermodal and international trade corridor," pointing out that any plan to secure cargo safety must start when the cargo is loaded by the manufacturer or when the container is put onto the vessel at a foreign port. This recognition of the importance of moving security efforts beyond U.S. territorial lands and waters is reflected in much of the post-September 11 effort to reduce the vulnerability posed by international waterborne shipping.

Thus, even before the summer of 2001, a number of ideas for improving seaport security had been proposed. These included developing port security plans, developing new methods of tracking cargo, pushing the borders of the United States out and sealing the supply chain, designating a lead agency for port security, and using public-private partnerships to carry out some of these tasks. The various efforts generating these ideas culminated in Senate Bill 1214, introduced by Senator Ernest F. Hollings in July 2001, and cosponsored by Senator Bob Graham. This bill formed the heart of the Maritime Transportation Security Act, signed November 25, 2002.

Current Port Security Measures

Federal policy initiatives in this arena have three aims.[8] First, they are designed to identify and reduce the vulnerabilities of port facilities and infrastructure and of the vessels in seaports. Second, they attempt to secure the cargo flowing through seaports. And third, they enhance awareness of the entire maritime domain—not just America's navigable

[8]Wrightson (2005a).

waterways, seaports, coastal waterways, and ocean coastal areas but also the entire global maritime environment.

Within each of these areas are numerous programs and initiatives. Among the most important are MTSA, the Container Security Initiative, and the Customs-Trade Partnership Against Terrorism. MTSA provides the overall planning and response framework. CSI places U.S. customs officials at foreign ports and has reporting requirements for cargo bound by ship for the United States. It is intended to interdict weapons of mass destruction and other terrorist threats before they arrive at U.S. ports. C-TPAT is designed to more closely control the movement of goods between their foreign source and final U.S. destination by enlisting the private trade community to secure its own supply lines.

Other elements of U.S. port security measures include a program to test new technologies (Operation Safe Commerce), the creation of a vessel identification and tracking system, the development of systems to target risky cargo for inspection, fostering of new security-related technologies, inspections of foreign ports, and a federal grant program aimed at providing an incentive to facilitate spending by ports and the private sector. An additional effort is taking place at the international level—the implementation of a new International Ship and Port Facility Security Code, adopted in December 2002 as amendments to the Safety of Life at Sea (SOLAS) Convention.

Maritime Transportation Security Act of 2002

The majority of these post-September 11 laws, rules, regulations, and programs have their origin in MTSA. Among other steps, the act required

- The creation of national, area, facility, and vessel security plans;
- The identification by federal authorities of vessels and U.S. facilities at risk;
- The creation of vessel and facility response plans;
- Transportation security cards for people who have access to vessels and facilities and crewmember identification cards;
- The creation of rapid-response maritime safety and security teams;

- An assessment of antiterrorism efforts at foreign ports;
- The placement of automatic identification systems on vessels in U.S. waters and a long-range vessel tracking system;
- The development of a program to evaluate and certify secure systems of international cargo shipment; and
- A new grant program (described below).

The Coast Guard has primary responsibility for implementing these measures. In fact, the Coast Guard reacted quickly even before MTSA was passed and implemented a Port Security Assessment Program, with expenditures starting in November 2001.[9] The program was designed to have the Coast Guard assess port vulnerabilities and security measures at the nation's 55 most important ports. Although the program continued after MTSA passage, the advent of MTSA led to changes in the assessment program.

MTSA has a high estimated price tag and even higher estimated benefits (Table 7.1). The Coast Guard estimated that implementation and continued fulfillment of the rules would cost more than $7.3 billion in 2003 dollars.[10] This estimate is computed at Maritime Security (MARSEC) level one, the lowest of three levels. Raising the MARSEC level to two twice a year for 21 days each time would raise the estimated cost by $6.6 billion. Costs were not estimated for MARSEC level three, the highest, and neither were opportunity costs computed, such as the time used for compliance rather than for other tasks.

The estimated benefits of $10.6 trillion roughly equal U.S. gross domestic product (GDP), a measure of the size of the U.S. economy. Assessing the accuracy of these figures is extremely difficult, especially because the process by which they were arrived at is somewhat murky.

---

[9]U.S. Government Accountability Office, 2004c.

[10]A GAO review of these cost estimates said that they should be treated with caution. Although they were made in good faith, a large number of uncertainties could create a wide range of error (U.S. Government Accountability Office, 2004a).

Table 7.1

Estimated Costs and Benefits of MTSA Measures
($ millions)

	Vessel Security	Facility Security	OCS Facility Security	AMS Plans	AIS	Total
First-year cost	218	1,125	3	120	30	1,496
First-year benefit	781,285	473,659	13,288	135,202	1,422	1,404,856
10-year present value cost	1,368	5,399	37	477	26	7,307
10-year present value benefit	5,871,540	3,559,655	99,863	1,016,074	10,687	10,557,819

SOURCE: *Federal Register (*2003), p. 60467.

NOTES: OCS is outer continental shelf. AMS is area maritime security. AIS is automatic identification system, the technology ships must install so that they can be identified.

However, they could be close to accurate if some type of highly catastrophic event were likely—such as a multiple detonation of nuclear devices at U.S. ports—and if MTSA measures had a high probability of stopping the event.

A rough evaluation of the costs of improving security for California ports has been undertaken. The major upgrades needed at some of California's busiest ports include worker identification systems, terminal traffic controls, surveillance and monitoring equipment, and utility upgrades. The costs associated with installing this equipment at ports in Oakland, San Francisco, Port Hueneme, Los Angeles, and Long Beach run in excess of $305 million.[11] Although not explicitly linked to MTSA, these costs were linked to program mandates by Congress, the Coast Guard, and other agencies. At the time the cost estimates were made, MTSA provided most of the requirements. Beyond California, according to a survey of U.S. ports, the implementation of the security

[11]Respectively, Oakland, $55 million; San Francisco, $70 million; Hueneme, $660,000, Los Angeles and Long Beach, $79 million (California Marine and Intermodal Transportation System Advisory Council et al., 2003).

measures mandated by the Department of Homeland Security (DHS) will take 20 years at current funding levels.[12]

Because of its complexity, different parts of the law are being implemented along different schedules. In addition, Congress is making changes along the way. We describe several different aspects of MTSA below.

Security Plans

Mandatory security planning for deterring and responding to a transportation security incident forms the core of MTSA.[13] At the heart of the mandated national maritime transportation security plan—in process but not yet finalized as of early February 2006—is the assignment of duties and responsibilities among federal agencies and the coordination of their efforts with state and local agencies. The national plan is to delineate a system of surveillance and notices to ensure the timely dissemination of information to the appropriate agencies whenever an incident occurs or is likely to occur. Finally, it is to define localities requiring area maritime transportation security plans.

The Coast Guard has developed 43 area maritime transportation security plans, assisted by area maritime security committees comprising government officials and industry and labor officials connected with maritime transportation.[14] These plans describe the area and infrastructure covered and how that infrastructure is integrated with the plans for other areas; they must be updated every five years.

A third level of security planning requires that owners and operators of ships and facilities submit independent plans with a focus on deterring a security incident. Unlike the national plan, MTSA does not specify that the vessel and facility plans should have a response component, although they are to be consistent with the national and area plans and are also to be updated every five years. Coast Guard regulations do

---

[12]Rosen Lum (2003).

[13]MTSA defines "transportation security incident" as a security incident resulting in significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

[14]Hereth (2004).

specify the need for response procedures. An estimated 12,700 plans were filed by the deadline of July 1, 2004, when they were to go into effect. These included 3,119 facility plans and 9,580 vessel plans. In a measure of quality control, the Coast Guard then completed on-site inspections of these plans by July 1, 2005.

Transportation Worker Identification Credential

Identification cards for port workers stem from several legislative initiatives. Partly in response to the Aviation and Transportation Security Act of 2001 and the USA PATRIOT Act of 2001, the U.S. Department of Transportation began to develop a transportation-sector access control card, now known as a Transportation Worker Identification Credential.[15] The Transportation Security Administration (TSA), then part of the Department of Transportation but later transferred to DHS in March 2003, was responsible. About one year after the other two laws, MTSA Section 70105 required that DHS develop a biometric identification card for ports and vessels. This responsibility also fell to TSA, which decided to use the transportation card system it was developing as the MTSA-required maritime card.

Meant for all transportation workers requiring unescorted access in secure areas of seaports, airports, and other transit facilities, these cards have followed a phased introduction. TSA started phase one, planning, in 2002. Phase two, the technology selection phase, followed. In August 2004, TSA announced the start of phase three, the prototype phase, in which the new ID card would be tested for seven months at four locations in the northeast, at the ports of Los Angeles and Long Beach, and at 14 major port facilities in Florida.[16] Participation during this phase was to be voluntary, and the actual use of the prototype card started in November 2004, with the Long Beach container terminal the first site. After a further review, TSA and the U.S. Coast Guard were to

---

[15]U.S. Government Accountability Office (2004d). The USA PATRIOT Act is Public Law 107-56, signed October 26, 2001. The acronym stands for United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. The Aviation and Transportation Security Act is Public Law 107-71, signed November 19, 2001.

[16]U.S. Department of Homeland Security (2004a).

move the card to phase four, its final phase, a nationwide rollout. However, this rollout may not occur until the end of 2006.[17]

International Policies

Parallel with MTSA, the International Maritime Organization has instituted a new set of rules for all countries and companies to follow, adopted in December 2002.[18] These rules included changes to the SOLAS Convention, and a two-part ISPS Code. Like MTSA, they went into effect on July 1, 2004.

Together, the measures required that governments set security levels and institute security measures appropriate to each level and complete port facility security assessments and plans for each facility. Ships had to carry out security assessments and develop security plans to be approved by the country under which they are registered. The measures also required that ships install automatic identification systems and ship security alert systems and create a permanent display of ship identification numbers.

A voluntary section of the ISPS Code calls for vessels to carry certain safety equipment, such as a hand-held metal detector and five hand-held radios. The United States is interpreting this voluntary section as mandatory for vessels bound for the United States.

In the first six months since the ISPS Code was in effect, the Coast Guard conducted more than 6,000 security examinations of vessels, including 831 in the district that includes California ports.[19] For the full year of implementation, July 2004 to June 2005, the Coast Guard took major control actions against 122 ships. These are cases where the Coast Guard detains a ship, denies it entry into a port, or expels it from a port because of security concerns or lapses. More than a third of these cases occurred in July 2004, the first month of implementation.[20]

---

[17]"TWIC Awaits TSA Standards" (2005), p. 10.

[18]This information is drawn from Crist (2003).

[19]U.S. Coast Guard (2005a).

[20]U.S. Coast Guard (2005b).

The Container Security Initiative

Whereas the Coast Guard is the lead agency with MTSA, Customs and Border Protection has taken the lead on CSI and C-TPAT. The concept for the CSI was first presented on January 17, 2002, by Customs and Border Protection Commissioner Robert C. Bonner in a speech at the Center for Strategic and International Studies. CSI is based on the idea of pushing U.S. border controls beyond actual U.S. borders and intercepting dangerous cargo before it arrives in the United States. It is best known for inspecting high-risk containers at foreign ports. The program consists of four core elements:

- Using intelligence and automated information to identify and target high-risk containers;
- Pre-screening containers identified as high-risk, at the point of departure;
- Using detection technology to quickly pre-screen high-risk containers; and
- Using smarter, tamper-evident containers.

As of December 2002, all ocean carriers were required to electronically transmit their manifests to Customs and Border Protection 24 hours before the cargo was to be loaded on the ship.[21] The manifest includes the contents of each shipment, the identity of the importer, and other information but is not necessarily verified by the company that operates the ship transporting the cargo. Officials at the port of embarkation, if it is a CSI port, the port of destination, and at the National Targeting Center in Virginia review this and other information, and the National Targeting Center analyzes the information in an automated targeting system. High-risk containers are then usually inspected at the foreign port by host-country customs officers but are sometimes inspected only on arrival in the United States.

The CSI has been implemented in two stages. In the first stage, arrangements were made with 23 ports—three Canadian ports and then

---

[21]This is the so-called 24-hour rule, which went into effect December 2, 2002, and became fully enforced on February 2, 2003. Although not specifically part of the CSI program, it is linked with it.

the 20 largest overseas source ports for maritime trade with the United States—to implement the inspection process. These ports, listed in the top panel of Table 7.2, are the source of 68 percent of all container traffic into the United States. All were operational as CSI ports as of the end of July 2005. A second round of negotiations resulted in the addition of the ports named in the second panel, increasing coverage to 80 percent of all container traffic into the United States. All but three of those were operational as CSI ports as of the end of 2005. Five others, not in phases one or two, had become operational as well, bringing the total to 44 ports by May 2006. Phase three of the CSI is to focus on capacity building at higher-risk ports.[22]

The eligibility of entry into the CSI program for foreign ports is subject to a set of fairly onerous conditions, making it unlikely that complete coverage of all sources of containers is achievable. [23] In fact, a requirement that the candidate port must have regular, direct, and sustainable container traffic to ports in the United States appears to rule out the notion of complete coverage altogether. There are some 2,600 commercial ports in the world, of which 575 handle significant numbers of containers.[24]

The Customs Trade Partnership Against Terrorism

C-TPAT is a joint government-business initiative to build cooperative relationships that strengthen overall supply chain and border security. Through this partnership, the U.S. government asks businesses to develop security procedures designed to maintain the integrity of their shipments and to have these procedures certified by the government. The program builds on previous joint programs instituted to battle the drug trade.

Businesses must apply to participate in C-TPAT and in so doing, commit to the following actions:

---

[22]U.S. Office of Management and Budget (2004).

[23]U.S. Customs and Border Protection (2004a).

[24]See www.lloydsports.com.

Table 7.2

Foreign Ports Participating in the CSI

Ports	Operational Date
Phase I Ports	
Algeciras, Spain	July 30, 2004
Antwerp, Belgium	February 23, 2003
Bremerhaven, Germany	February 2, 2003
Felixstowe, United Kingdom	May 24, 2003
Genoa, Italy	June 16, 2003
Halifax, Canada	March 1, 2002
Hamburg, Germany	February 9, 2003
Hong Kong	May 5, 2003
Kaohsiung, Republic of China	July 25, 2005
Kobe, Japan	August 6, 2004
La Spezia, Italy	June 23, 2003
Laem Chabang, Thailand	August 13, 2004
Le Havre, France	December 2, 2002
Montreal, Canada	March 1, 2002
Nagoya, Japan	August 6, 2004
Pusan, South Korea	August 4, 2003
Rotterdam, The Netherlands	September 2, 2002
Shanghai, People's Republic of China	April 28, 2005
Shenzhen, People's Republic of China	June 24, 2005
Singapore	March 10, 2003
Tokyo, Japan	May 21, 2004
Vancouver, Canada	March 1, 2002
Yokohama, Japan	March 24, 2003
Phase II Ports	
Barcelona, Spain	Not yet operational
Colombo, Sri Lanka	June 29, 2005
Durban, South Africa	December 1, 2003
Gioia Tauro, Italy	October 31, 2004
Gothenborg, Sweden	May 23, 2003
Liverpool, United Kingdom	November 1, 2004
Livorno, Italy	December 16, 2004
Marseilles-Fos, France	January 7, 2005
Naples, Italy	September 30, 2004
Osaka, Japan	Not yet operational
Port Kelang, Malaysia	March 8, 2004
Southampton, United Kingdom	November 1, 2004
Tanjung Pelepas, Malaysia	August 16, 2004
Thamesport, United Kingdom	November 1, 2004
Tibury, United Kingdom	November 1, 2004
Valencia, Spain	Not yet operational
Zeebrugge, Belgium	October 2, 2004

Table 7.2 (continued)

Other Ports	
Buenos Aires, Argentina	November 17, 2005
Cortes, Honduras	March 25, 2006
Dubai, United Arab Emirates	March 26, 2005
Lisbon, Portugal	December 14, 2005
Piraeus, Greece	July 27, 2004
Santos, Brazil	September 22, 2005
Salalah, Oman	March 7, 2006

SOURCES: Flanagan (2003); U.S. Customs and Border Protection (2004b); and U.S. Customs and Border Protection press releases, various dates.

NOTES: Only the Port of Yantian is included in CSI coverage of Shenzhen. Shenzhen also includes the ports of Shekou, Chiwan, and other, smaller ports. The table is current as of the beginning of May 2006.

- Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines, jointly developed by Customs and Border Protection and the trade community. These guidelines encompass procedural security, physical security, personnel security, education and training, access controls, manifest procedures and conveyance security;
- Submit a supply chain security profile questionnaire to Customs and Border Protection;
- Develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines; and
- Communicate C-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies.

These plans are distinct from the plans required under MTSA. As such, they extend security planning from ports, other maritime facilities, and ships—for which planning is mandatory—to the entire supply chain outside the United States, from the foreign loading dock to the U.S. border or seaport. Unlike with the MTSA requirements, no federal

money, either through formulas or grants, is available to private companies that participate in C-TPAT.

As with the other programs, C-TPAT rolled out in phases. The first phase included major importers. The next opened the program to global transportation companies, and the third opened the program to brokers, freight forwarders, and non-vessel-owning common carriers. Port authorities, terminal operators, and selected foreign manufacturers are now also included. By the end of 2005, nearly 10,300 companies had applied, covering well over 50 percent by value of maritime cargo. Of those applicants, more than 5,600 had been accepted for membership. Membership is encouraged by the promise of reduced inspections and therefore reduced border wait times.

Other Customs and Border Protection Programs

Aside from CSI and C-TPAT, Customs and Border Protection has at least five other efforts as part of a layered strategy to protect the global supply chain.[25] As noted above, the 24-hour rule is one of these, requiring that ocean carriers send their manifests to Customs and Border Protection 24 hours before the cargo is loaded on a ship at a foreign port. A second is the placement of non-intrusive inspection technology, such as x-ray or gamma-ray machines, at ports and borders to take an image of the content of boxes. A third is the placement of radiation detection equipment, such as radiation portal monitors (RPMs), at seaports with the intention of screening every container entering the United States. RPMs had been placed at the Port of Oakland by February 2005 and were unveiled at the ports of Los Angeles and Long Beach in July 2005.

The use of dogs trained to detect explosives, chemicals, narcotics, people, biological agents, and agricultural pests is another effort. Finally, Customs and Border Protection is also participating in efforts to make shipping containers more secure, including redesigning them, making

---

[25]Adams (2005). At the time of this testimony, Adams was acting director of field operations for Customs and Border Protection in Los Angeles, responsible for the seaports of Los Angeles, Long Beach, and Port Hueneme and the airports at Las Vegas, Los Angeles, Ontario, Palm Springs, and Victorville, the Southern California Logistics Airport.

them harder to break into, instituting higher standards for seals, and developing sensors that will detect tampering.

Federal Port Security Grants

Estimates for implementing new port security measures placed costs in the billions of dollars. To defray some of these costs, the federal government instituted port security grants in the Department of Defense Appropriations Act of Fiscal Year 2002, even before MTSA.[26] They were then written in to MTSA, but Congress continued to fund the grants under the terms of the earlier Defense appropriations act, rather than under the terms of MTSA.[27]

As of September 2005, DHS had awarded $779 million in port security grants (Table 7.3).[28] Most have been distributed through the Transportation Security Administration, with $75 million distributed through the DHS Office of Domestic Preparedness (ODP). The TSA grants have been awarded in five separate rounds under the Port Security Grant Program, with the fifth concluded in September 2005, and three rounds under Operation Safe Commerce. ODP grants were distributed in a single round. In 2004, starting with round five, DHS placed the TSA Port Security Grant Program in the newly created Office of State and Local Government Coordination and Preparedness (SLGCP), which includes ODP. SLGCP was subsequently changed to the Office of Grants and Training.

In 2003, California ports handled 36 percent of all U.S. waterborne imports and 49 percent of all waterborne containerized imports by value. They handled a much smaller proportion of the weight of national imports (10.7%), but 39.9 percent of containerized imports by weight. Despite the proportion of trade they handle, California ports and others in the maritime industry received only 19 percent of all federal port-security-related grant money between the start of the grant programs in 2002 and the fifth round in 2005.

---

[26]This appropriations act was Public Law 107-117, signed January 10, 2002.

[27]U.S. Department of Homeland Security (2005).

[28]This figure includes $92.3 million awarded in June 2002, before the existence of DHS. Alternative sources give a figure of $623 million in total grants.

Table 7.3

Federal Port Security Grants

Program	Date	U.S. Amount ($ millions)	California Amount ($ millions)	California Share (%)
Port Security Grant Program				
Round 1	June 2002	92.3	17.1	18.5
Round 2	July 2003	169.1	30.2	17.9
Round 3	December 2003	179.0	33.7	18.8
Round 4	September 2004	49.4	5.9	11.9
Round 5	September 2005	142.0	33.6	23.7
Total awarded		631.8	120.5	19.1
Office of Domestic Preparedness, Urban Areas Security Initiative				
	May 2003	75.0	9.1	12.1
Operation Safe Commerce				
OSC-NE	N/A			
OSC 1	June 2003	28.3	8.3	29.3
OSC 2	July 2003	26.7	5.4	20.2
OSC 3	April 2005	17.1	6.7	39.2
Total awarded		72.1	20.4	28.3
Grand total		778.9	150.0	19.3

SOURCE: U.S. Department of Homeland Security, various documents.

The Port Security Grant Program

In the initial round, the Transportation Security Administration was charged with disbursing $93 million through a competitive grant program to assist critical national seaports in financing the costs of facility and operational security enhancements. TSA worked with MARAD and the Coast Guard to develop the grant process and to select the projects for the awards. Grants were awarded for one of three broad categories: (1) to conduct security assessments and develop strategies for filling security gaps, (2) to enhance facility and operational security, for example, to pay for equipment for facility access control, communications, surveillance, cargo security, and passenger security, and (3) to finance proof-of-concept demonstration projects, meaning projects that explore the use of new technologies.

As mandated under MTSA, the agency developed the TSA Maritime Self-Assessment Risk Module (TMSARM), a vulnerability self-assessment tool. This lessened the need to give grants in round two for the first category, security assessments, and mitigation strategies.[29] Furthermore, in rounds three and four, grants were awarded only for the second category, enhanced facility and operational security.[30]

In selecting grantees, preference has been given to single terminal- or facility-specific projects rather than to portwide projects.[31] However, projects that enhance intermodal transportation security within the footprint of the port have also been given preference. The Transportation Security Administration and DHS have preferred projects that address access, command, control, coordination and communication, and physical security and has also emphasized projects that focus on prevention, deterrence, and detection rather than consequence management.

Operation Safe Commerce

OSC funds pilot programs that are meant to enhance and complement other security initiatives, such as C-TPAT and CSI, by testing technologies and business processes that protect commercial shipments from tampering all along the supply chain, from point of origin to point of destination. For a project to be funded, it must accomplish one or more of the following tasks to secure the supply chain:

- Validate security at the point of origin, to include the security of the shipment itself and the information that describes it;
- Secure the supply chain from the point of origin to its final destination and all the points in between; and

---

[29]TMSARM is intended to assist company security officers, vessel security officers, and facility security officers in conducting assessments of vessels and facilities.

[30]The federal government is funding other proof-of-concept projects, such as biometric IDs and other technologies, under separate MTSA programs.

[31]An example is a project that focuses on increasing security at a particular terminal, as opposed to a project to construct a new fence all around the whole port.

- Monitor the movement and integrity of the cargo while in transit using available technology.[32]

OSC started with a pilot program called Operation Safe Commerce-Northeast, now known as the Canada-U.S. Cargo Security Project, launched in August 2001, actually before the events of September 11.[33] In OSC-NE, state and federal agencies joined with private companies to develop effective security models for international shipping systems.[34] The goal was to improve security practices by using point-of-origin security, in-transit tracking and monitoring, and data query capabilities to facilitate commerce while improving security. During the first phase of OSC-NE, DOT chose commercially available technology to track and monitor an individual container with 400,000 automotive tail lamps as it made its way from Slovakia to Hillsborough, New Hampshire.[35]

After this demonstration, TSA instituted OSC proper for the three largest container load centers—the port complexes of Los Angeles and Long Beach, Seattle and Tacoma, and New York and New Jersey. The program has had three funding rounds, with a total of $72.1 million awarded; about 28 percent went to projects associated with the ports of Los Angeles and Long Beach.

---

[32]OSC does not provide funding for research and development projects. Instead, it encourages the use of commercial-off-the-shelf technology, emerging technologies, and processes that have been tested and are readily available to the public.

[33]A very detailed timeline of the project is available from the NI2 Center for Infrastructure Enterprise at http://www.ni2cie.org/cuscsp/timeline.asp.

[34]The following agencies and companies were involved in the project: Immigration and Naturalization Service (Border Patrol), U.S. Marshall Service, U.S. Attorney Offices in New Hampshire and Vermont, Coast Guard, and U.S. Customs Service. Participants from the private sector included Sylvania/Osram, BDP International, and C.P. Ships. The Port of Montreal and the New Hampshire International Trade Association were also involved in the project (Sylvania/Osram news releases, available at http://www.sylvania.com/press/06142002.html).

[35]The container left Nove Zamky, Slovakia, on May 22, 2002, and arrived via land to the Port of Hamburg, Germany, where it was loaded onto a Canada-bound ship. It arrived at the Port of Montreal on June 3. The container was then loaded onto a truck. It crossed the border from Quebec to Vermont at the Highgate Springs border crossing. It then traveled through Vermont before arriving at Hillsborough, New Hampshire, on June 7.

ODP Port Security Grants

ODP, originally part of the Department of Justice, then part of DHS, and now housed within the DHS Office of Grants and Training, provides training, money, and other assistance to state and local governments.[36] Accordingly, ODP launched the Urban Areas Security Initiative (UASI) in 2003 to provide financial assistance to large urban areas to increase their level of preparedness. In early 2003, Congress appropriated $700 million to fund discretionary grants under UASI. In selecting projects for funding, Congress instructed ODP through DHS "to take into consideration credible threat, vulnerability, the presence of infrastructure of national importance, population, and identified needs of public agencies." Consequently, one component of the UASI was a port security program.

The guidelines for selecting projects for the UASI port security program were the same as those for the more general port security grants, and grantees for this program were selected from a pool of applicants that had previously applied for those grants. However, the UASI port security program was more restrictive in that only applicants from selected urban areas were eligible. At the same time, it was less restrictive in that up to 10 percent of the gross amount of the award could be applied to operational expenses associated with increased security measures during three specific orange threat alert levels, the fourth-highest of five alert levels in the U.S. homeland security alert system, which took place during the first half of 2003. In May 2003, ODP announced $75 million in grant awards under the UASI Port Security Grant Program, funding 85 projects ranging in cost from $10,000 to $3.5 million at 15 different U.S. ports.[37]

R&D Grants

Aside from the more general port security grants, MTSA instituted research and development grants aimed mostly at technologies. The bill

---

[36]For more information, see http://www.ojp.usdoj.gov/odp/ (as of June 24, 2004).

[37]A complete list of all the grants awarded is available at www.ojp.usdoj.gov/docs/fy03uasi_psg.pdf.

authorized $15 million for each fiscal year from 2003 through 2008. The money was aimed at the development of

- Targeting and inspection methods;
- Equipment to detect explosives, chemical or biological agents, and nuclear materials;
- Container tags, seals, and tracking sensors;
- Tools to mitigate the consequences of a terrorist act at a port; and
- Ways to apply existing technologies to port security.

The Coast Guard and Maritime Transportation Act of 2004 broadened the scope of activities these grants could fund. In particular, it requested the development of technologies to track activities in marine areas, known as maritime domain awareness; improved container design, including blast-resistant containers; and methods (rather than new technologies) to improve the security and sustainability of ports in case of a terrorist incident. The money authorized for this was raised to $35 million annually from 2005 to 2009. The bill also provided for the establishment of national port security centers at U.S. universities, along the lines of new homeland security research centers that have been established.

In some ways, the bill represents learning by policymakers, as exemplified by the new allowance for maritime awareness technologies. After MTSA, and after the Coast Guard was required to devote more resources to understanding port security and developing new plans and capabilities, maritime domain awareness rose in importance. This was especially true because the maritime environment has vulnerabilities other than ports, such as nuclear plants, chemical plants, and even the locks on inland navigable rivers.

Evaluating Port Security Policies

Faced with an unfamiliar and highly risky situation—protecting America's ports and global supply chains from terrorist attacks—the U.S. and local governments have quickly developed a number of programs. How well do these programs serve their purpose?

An evaluation of port security policies may be divided into four areas. The first is whether policies optimize security programs, resources, and activities. Are the measures instituted appropriate, in the sense of getting the most security for their cost and directing assets optimally? The second is the effectiveness of programs. If fully complied with, will the plans and programs improve security? Will they in fact be complied with? Related to this is the cost-benefit balance. Even if the programs are only partially effective, they may be worthwhile if they are low cost. In contrast, even very effective but extremely costly programs may not be worthwhile. Third is the issue of unclear authority and priorities. In the sprint to create security measures, a number of laws covering the same issues were passed but not necessarily coordinated, and agencies were tasked with quickly obeying legislative mandates. Last is the issue of financing. Who is to pay for all of this?

Optimizing Security Programs, Resources, and Activities

Optimizing programs, resources, and activities is perhaps the most difficult because it requires a fully informed understanding of the threats, the probabilities of those threats occurring, the benefits of stopping such events, and the costs of stopping them. Devoting staff time to sealing the supply chain might mean devoting less staff time to creating identification cards. Complicating this is the fact that port security is but one piece of homeland security, and hardening the ports and the maritime transportation system might make another target, such as sports events or shopping malls, even more inviting.

Designing port security programs therefore can be viewed as following a simple decision structure (Figure 7.1). At the top level is the decision of how much effort to devote to maritime security as opposed to airport, communications infrastructure, rail transport, or energy infrastructure security. The next level, given the decision on maritime security, divides that effort between ports and the supply chain and other vulnerabilities in the maritime domain, such as oceanside nuclear plants and locks on inland waterways. The United States has to be wary of

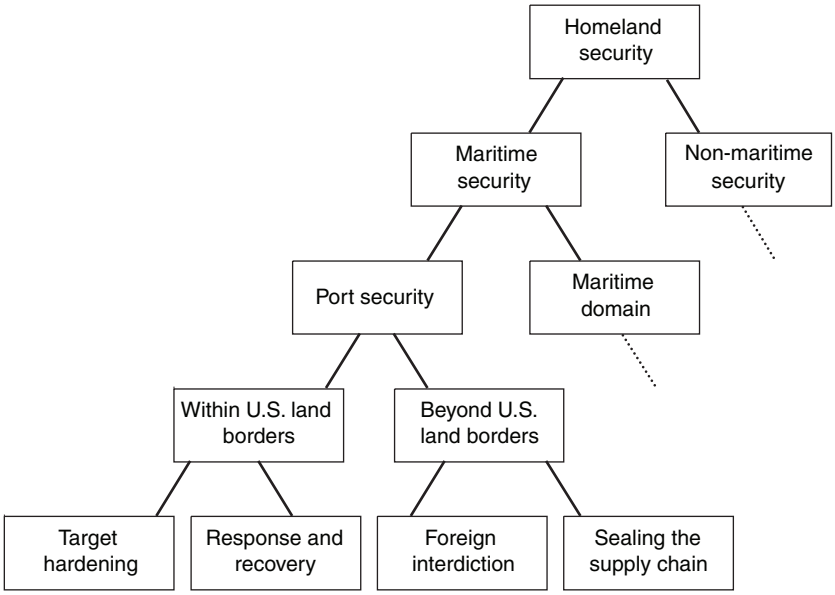


Figure 7.1—Port Security Decision Structure

threats along 12,375 miles of coastline and 25,000 miles of river or inland shoreline.[38]

The next decision level then focuses on whether to put attention into the ports within U.S. borders or into actions and programs outside the United States. The former actions include placing non-invasive inspection equipment at U.S. ports, strengthening access controls, or improving security planning. The latter actions include CSI and C-TPAT.

Next, with attention devoted to domestic programs, security planners must balance preventing incidents with establishing protocols for responding to incidents and recovering from them. Assuming that absolute prevention of an incident is an impossibility, it would be tragic to invest vast resources in prevention only to see U.S. commerce paralyzed following an incident, with no clear plan on how to quickly reconstitute the flow of goods. The final decision involves allocations

[38]U.S. Government Accountability Office (2004b).

within the chosen categories. Focusing just on prevention efforts at ports, for example, key issues include whether all ports should reach some minimum standard, whether larger ports should get a disproportionate share of funding and attention, or whether all ports should be treated equally in terms of responsibilities and grant competitions.

Given the multiplicity of choices and the constrained resources, the U.S. Government Accountability Office, the nation's chief fiscal and program watchdog, recommends that the United States allocate its security resources using a risk-management approach.[39] This includes assessments of threat (the likelihood of terrorist activity against an asset), vulnerability (the asset's weaknesses), and criticality (the relative importance of the asset). Shortly after taking over as head of the Department of Homeland Security in early 2005, Michael Chertoff articulated the adoption of a risk management strategy for the department.[40]

Although this approach may be best, implementation will not be easy because each element is difficult to quantify. The strategic intentions of U.S. terrorist adversaries are relatively well known, but their tactical intentions are less well known, and so it is impossible to know whether the United States has allocated its maritime security resources optimally. It is fair to say, however, that evidence indicates that it could be doing better. To illustrate the choices facing policymakers, we consider prevention versus recovery, the port security grant program, the inclusion of labor, and the balance between the East and West Coasts.

Prevention Versus Recovery

Much of the effort so far has been tilted toward prevention rather than recovery. The trade community has put its weight behind wanting more recovery planning; the analyses in other chapters of this volume support this request. Certainly, some work has been done already. For example, the Department of Homeland Security has a national response plan, California has an oil spill contingency plan (which could provide

---

[39]Decker (2001).

[40]Chertoff (2005a, 2005b).

an input into a state response plan to a terrorist incident), and ports themselves are developing plans, such as a newly developed plan to reopen the ports of San Francisco Bay after a maritime security incident.[41]

However, policymakers and the trade community at large remain uneasy about how the maritime system as a whole will be reconstituted. At a national cargo summit in December 2004, private sector participants indicated that they remained uninformed about possible federal actions after an attack and voiced their preferences for taking part in contingency planning under a variety of scenarios.[42] At the same summit, Bonner of Customs and Border Protection said that a continuity of trade plan is being developed by the Coast Guard and his agency.

The U.S. Coast Guard and partner agencies engage in extensive exercises to test aspects of the Coast Guard's terrorism response plans. A GAO analysis of 85 exercises carried out from October 2003 to September 2004 identified four groups of problems that these exercises revealed. These included communication problems among different agencies, inadequate and uncoordinated resources, a lack of knowledge or training in the incident command structure, and lack of knowledge about who has jurisdictional authority.[43] These exercises are continuing.

The Grants Program and Labor

The grants program and the handling of labor both illustrate the question of allocations within security categories. Grants cannot be used for the operation of equipment or for training of personnel and must be spent within one year. Port officials consider these terms too rigid. Any

---

[41]For the national plan, see U.S. Department of Homeland Security (2004b). For the state's oil spill response, see California Department of Fish and Game (2003). The San Francisco Bay plan was presented to the Northern California Area Maritime Security Committee on July 12, 2005.

[42]Homeland Security Institute (2005). Willis and Ortiz (2004) also note a lack of emphasis on what they call "fault tolerance"—making sure an attack on one part of the system does not bring down the whole system—and resilience—making sure the system can be brought back into operation quickly after an attack.

[43]U.S. Government Accountability Office (2005a).

new security equipment must be maintained and, often, security-enhancing projects can take more than a year to complete. The choice between the purchase of equipment and the maintenance of that equipment is an allocation decision that fits within the framework described above.[44]

Properly targeting grants has been an issue throughout the development of the U.S. homeland security response. In an evaluation of the federal grant system for first responders, the GAO reported that any effective grant system should target states and localities at greatest risk. "A proclivity to spread money around, unfortunately, may provide less additional net protection while actually placing additional burdens on state and local governments. Given the significant needs and limited federal resources, it will be important to target to areas of greatest need."[45]

The involvement of labor provides another illustration of allocation choices, this time in terms of where program requirements and staff attention are directed. As of early 2004, West Coast dockworkers had expressed great concern about the types of background checks that might be needed for maritime industry identification cards. Certainly, without dockworker cooperation, global supply chains could remain vulnerable to terrorist infiltration. Yet even by 2005, and even with the development of the TWIC, it is not clear that labor is as involved in port security planning and programs as it should be. The Transportation Security Administration does not appear to have identified how to sustain the support of port workers in its TWIC program.[46] Regarding another group of workers, one representative of the International Brotherhood of Teamsters noted in early 2005 that many truck drivers, who move containers into and out of ports, were poorly paid immigrants—not necessarily in the United States legally—vulnerable to being used by

---

[44]A number of port officials discussed the rigidity of the federal grants program in testimony at a hearing entitled, *Security and California Ports*, sponsored by the Office of California State Senator Christine Kehoe, the California Office of Homeland Security, and the California Association of Port Authorities, and held in Sacramento, California, on February 16, 2005.

[45]Posner (2003), p. 14.

[46]U.S. Government Accounting Office (2004d), p. 16.

potential terrorists. Even given the vested interest of the Teamsters in port trucking, federal and state programs do not appear to have fully considered how to include truckers, warehouse workers, and other port-related labor in port security planning, incident prevention, response, and recovery.

The West Coast faces a special labor issue that ports elsewhere may not face, suggesting that amicable labor relations might be even more important from Seattle to San Diego. Dock workers on the West Coast work under a single union, giving that union enormous bargaining power in the introduction of new technologies that could enhance port security. East Coast ports have many different unions, leading to site-specific dynamics in labor-management negotiations, agreements, and operations.

West Coast and East Coast

A final illustration of allocation issues, germane in particular to California, involves port security efforts on the West Coast versus those on the East Coast. There is some question as to whether the West Coast ports are receiving the appropriate protection. Although questions are raised, often by West Coast policymakers, it is not clear whether these are truly gaps or merely perceptions of gaps. Several examples are available.

The Coast Guard is currently implementing a long-term recapitalization plan known as the Integrated Deepwater System, meant to bring on new ships, helicopters, aircraft, and technology and information systems. It is doing so in part because its existing fleet of aircraft—helicopters and airplanes—and cutters—ships ranging in size from 110 feet to 378 feet—is extremely old. The Coast Guard on the West Coast depends on 378-foot cutters to a much greater extent than on other coasts. In fact, 10 of the Coast Guard's 12 378-foot cutters are deployed in the Pacific Area Command. They are on average 36.3 years old, have an estimated service life of 40 years, and are deteriorating. Current funding levels make it impossible for the Pacific Area Command to keep all 10 cutters fully mission capable, so the command has instituted a new program to improve maintenance practices and keep the cutters running through 2016, when they are to be replaced by new

National Security Cutters. As of mid-2005, it was difficult to know whether this new effort would be successful.[47]

Similar questions have arisen with the Coast Guard's airborne fleet, in particular its armed helicopters deployed in airborne use of force. The Coast Guard started flying armed helicopters around 1999; new armed helicopters were delivered in 2001 and the Coast Guard formally commissioned its first airborne use-of-force unit in Jacksonville, Florida, in 2003. In the last several years, the Coast Guard has started modifying and arming two types of helicopters in its existing fleet, and a set of these helicopters is operational in Atlantic City, New Jersey. In mid-2005, at a U.S. House of Representatives hearing, Representative Lucille Roybal-Allard of Los Angeles asked the question of concern for the West Coast: If the timeline for modifying and arming helicopters is not met, "what interim measures will the Coast Guard take to provide this type of airborne protection to critical coasts such as the Los Angeles–Long Beach port?" The response was that continued arming would depend on funding, but that San Diego was scheduled to receive a set of the modified, armed helicopters in 2005.[48]

Similar to the placement of airborne use of force capabilities is the placement of counterterrorism capabilities. As part of MTSA, the Coast Guard was called on to create maritime safety and security teams to deter and respond to terrorism, among other duties. It created 13 teams, but in January 2004 changed one of these—the Chesapeake team in Virginia—into an enhanced maritime safety and security team, described as "the Coast Guard's first dedicated counter terrorism unit."[49] Despite the vulnerability and importance of West Coast ports and the extra capabilities of these enhanced teams, it is as yet unclear whether any of the enhanced teams will be formed on the West Coast.[50]

---

[47]U.S. Government Accountability Office (2005d).

[48]Federal News Service (2005b).

[49]U.S. Coast Guard (2005c).

[50]U.S. House of Representatives (2005).

Effectiveness

The Department of Homeland Security has a simple goal in terms of cargo security. Specifically, it aims to correctly identify high-risk cargo and inspect 100 percent of it.[51] Unfortunately, there is no way to guarantee that the department will identify all high-risk cargo: "Simply put, there is no truly secure substitute for 100% checking of all cargo for WMD, particularly in light of the adaptive and shifting nature of terrorist strategies."[52] Unfortunately again, careful inspection of all cargo will wreak economic havoc. This leaves security planners in the difficult position of designing programs that will have high likelihoods of detection success. We might never know whether these programs are successful. Absence of detection and absence of a terrorist incident might simply mean that terrorists used other methods and pathways for their goals or that they succeeded in infiltrating a weapon but that it failed to work.

What we can ask is whether the programs, as designed, will perform as hoped for. There are reasonable doubts, in particular because of the reliance on voluntary commitments by people participating in the programs. Two Customs and Border Protection programs—C-TPAT and CSI—illustrate the issue.

In C-TPAT, participating companies complete a security profile, which Customs and Border Protection (CBP) reviews and certifies. Importers go through an additional certification step. If they pass, importers are given fewer cargo inspections and other benefits that may reduce the amount of scrutiny given their cargo.[53]

Only after benefits are granted, however, does CBP validate C-TPAT members to make sure they are, in fact, implementing their security measures. Before validation, CBP gives the member 30 days notice, and the two parties jointly determine what the validation

---

[51]U.S. Department of Homeland Security (2004b). By "inspect," DHS does not necessarily mean opening and unpacking the containers. Rather, inspection in most cases is to be accomplished by radiation detection, imaging, or other non-intrusive technologies.

[52]Homeland Security Institute (2005), p. 8.

[53]U.S. Government Accountability Office (2005b).

inspection will cover. However, it is not clear whether after validation CBP has plans to ensure participant compliance. This suggests that even with validation, CBP relies on the good faith of its C-TPAT members in the implementation of their security responsibilities. This faith may prove justified, given the screening and certification of all members and the additional validation for importers. But it may not, and there is no way to know. As of November 2004, CBP officials had validated—that is, actually made sure that security measures were being implemented—409 members out of more than 4,100 certified members and 7,300 applicants. Responding to criticisms regarding the pace of validations, CBP has hired additional inspectors. As of the end of 2005, 10,286 companies had applied for C-TPAT membership, with 5,636 accepted. Of those, 1,405 had been validated, and validations were under way for an additional 2,278 applicants.[54]

The C-TPAT program has one other flaw in its effectiveness. By creating a system in which some participants get less scrutiny, it makes it possible for these participants to learn how to game the system so that they can more easily smuggle something into the United States.[55] The problems of validation and system gaming do not necessarily invalidate the usefulness of C-TPAT. They suggest, however, that increased effectiveness will require a more serious validation effort and ways to make sure that participants cannot use their involvement in the program to smuggle weapons or people.

CSI presents similar coordination challenges regarding effectiveness. Under the program, CBP analyzes the manifest, reported by the ocean carrier, and other information provided by the importer at the National Targeting Center, at the port of embarkation, and at the U.S. destination port. CBP then decides whether a container is high risk and merits further inspection. This inspection is to take place at the port of embarkation. However, according to a recent analysis, only about two-thirds of containers coming through CSI ports were analyzed as to their

---

[54]Tirschwell (2006).

[55]Willis and Ortiz (2004).

risk, and 72 percent of designated high-risk containers were inspected at the foreign port.[56]

Not all containers are analyzed in part because of lack of proper staff to do so and in part because the manifest information is too low quality for effective analysis. Not all high-risk containers are screened because host-country officials may decide on the basis of their own information that the container is not high risk, or because the container was already loaded on a ship by the time it was deemed high risk. In cases where a high-risk container is not inspected, CBP can order the container to be inspected at the U.S. port. This occurs most of the time but defeats the purpose of CSI, which is to inspect high-risk containers *before* they reach the United States. CBP can also give a *do not load* order, and this has been given six times from the start of the program through early 2005.

Even an inspection at a foreign port might not be enough to find a hidden weapon. Foreign inspections are carried out by host-country officials either with non-intrusive inspection technology, such as some type of radiation detector, or physically. However, as of early 2005, there were no minimum technical standards for the inspection technology used at foreign ports. Even though CBP says that all inspection equipment at foreign CSI ports is at least as good as the equipment used at U.S. ports, the lack of minimum technical standards suggests that the United States does not have complete assurance that the foreign inspections will be effective.[57]

The CSI raises other effectiveness issues, in particular the ports selected and the coverage that selection gives regarding U.S. waterborne trade. The Customs and Border Protection agency and terrorists are reacting to each other as adversaries. The government must select ports from which dangerous materials are likely to come given that potential terrorists know that the government will be selecting ports from which dangerous materials are likely to come. Starting with the 20 largest might have been a good decision, but it made it more likely that other ports would be used by terrorists, something which the Customs and Border Protection needs to account for in its targeting strategies.

---

[56]U.S. Government Accountability Office (2005c).

[57]U.S. Government Accountability Office (2005c), p. 5.

The CSI ports that were operational as of January 1, 2006, accounted for 65.6 percent of U.S. containerized imports, by value.[58] The ports of Los Angeles, Long Beach, and Oakland each received more than 66 percent of their containerized imports by value from CSI ports.[59] However, in terms of number of ports, less than 3 percent of all ports that send containerized imports to the United States were CSI ports. For California, the proportion of CSI ports relative to all foreign ports originating containers shipped to any California port ranged from 5.1 percent for Los Angeles to 7.5 percent for Oakland among the big-three ports, with a statewide average of 4.3 percent.

Do these programs work? In January 2005, 32 Chinese nationals were found in two shipping containers at the Port of Los Angeles, spotted only because a crane operator—a worker perhaps not fully considered in U.S. port security planning—spotted three men climbing out of a container. They originated in the Port of Shekou, China—part of the Shenzhen port area—which had been designated for CSI status but not yet gone operational.[60] They arrived on the NYK *Athena*, a Panama-flagged ship owned by a Cyprus-based company but part of the NYK Line (Nippon Yusen Kaisha), a Japanese ocean carrier. The ship was fully compliant with its security obligations under the ISPS code and had International Ship Security Certificate 200400863. Could CSI targeting have discovered the men? To know with certainty is almost impossible.

Even if all of the port security programs are only partly effective, a final evaluation should include a balancing of the costs and benefits. Such an analysis would have to include the full costs of the programs—dollar outlays and opportunities forgone from spending the money on

---

[58]The import coverage is based on 2003 waterborne trade data.

[59]The recent additions of more ports to the CSI program in 2006 will not have changed these numbers much. The new CSI ports handle only a very small proportion of U.S. imports.

[60]"32 Stowaways Found on Ship" (2005), and Slater (2005). Shenzhen went operational on June 24, 2005, but the port is a complex of several areas and the operational portion reportedly included only the Yantian section, leaving Shekou still without CSI coverage.

these programs rather than for other purposes—and the full benefits—the extra security and potential economic efficiencies that they buy.

Unfortunately, little work has been done in this area. The Coast Guard has done its own analysis of just the MTSA measures (Table 7.1). The White House Office of Management and Budget has also looked at several MTSA measures, as well as other cargo security measures, but has not gone beyond agency evaluations. Instead, costs are those provided by the Coast Guard or Customs and Border Protection, whichever is applicable, and benefits are listed as "reduced risk from a transportation security incident" and "homeland security."[61] The Organisation for Economic Cooperation and Development (OECD) also looked at costs of various measures but declined to fully investigate benefits because of great uncertainties inherent in such estimates.[62]

The uncertainties arise because the threat of terrorism includes many unknown variables and many extremely low-probability events. Furthermore, necessary information (such as the effectiveness of programs and intelligence about terrorist plans and activities) is held by governments and not generally disclosed. This suggests that a comprehensive cost-benefit analysis can best be performed by the U.S. government or at least by some agency, organization, or researcher with full access to government information. At this time, such an analysis or effort is not known to exist but would be extremely useful for policy planners to have.

Unclear or Duplicated Authority and Lack of Priorities and Implementation

At least two important areas of port security—grants and identification cards—have unclear or duplicated authorization from within the federal government. Although these programs have proceeded, the conflicting authorizations suggest that they may not be doing so in the way policymakers intended. In addition to receiving unclear or duplicated authority, agencies received long but unprioritized lists of tasks. This multiplicity of tasks has been accompanied by the

---

[61]U.S. Office of Management and Budget (2005).

[62]Crist (2003).

failure to proceed in a timely way with programs, as in the case of securing cargo transport, implementing identification cards, and updating the Coast Guard's air and sea fleet. This has clearly been a concern to policymakers, although they have not always stepped in to clarify their instructions.

The port security grant program has two separate sets of rules and conditions. One set, used by the Transportation Security Administration when it administered the grant program, comes from the fiscal year 2002 Defense Appropriations Act. A second set comes from MTSA. Funding has been appropriated under the rules used by TSA, but TSA has adapted the program to MTSA requirements. The two funding mechanisms, as well as the programs, are different. For example, the TSA rules call for funding to be focused on critical national seaports and they do not require any cost share. The MTSA terms allow recipients to be port authorities, facility operators, and state and local agencies and call for a local cost share for most projects of greater than $25,000.[63]

A similar duplication has occurred with the transportation worker cards. These have now been delayed well beyond their planned rollout.[64] The Aviation and Transportation Security Act, the USA PATRIOT Act, and MTSA all provided in one way or another for these cards. Before being charged with implementing the MTSA-required card, TSA, working under the authority of the other two laws, decided that the card program would be done through a cost-sharing effort, in which the federal government would provide the biometric card and database and local entities would provide the equipment to read the card and control access. Once TSA took over the MTSA-required card, however, DHS directed it to explore the costs and benefits of three options—the federal-local approach, a pure federal approach, and a decentralized approach, in which ports would develop their own systems and issue their own cards in compliance with a federal regulation. The

---

[63]Information about these details of the port security grant program emerged in January 2005 (U.S. Department of Homeland Security (2005), pp. 13–16 in particular). It is not clear whether the issue of two sets of conditions has been resolved.

[64]U.S. Government Accountability Office (2004d).

need to evaluate these three options is one reason the program has been delayed.

This is not to say that TSA should not explore different options. Rather, moving in one direction—the federal-local option—and then regrouping to consider other options is a sign of unclear guidance in the various programs. In its analysis of this program, the U.S. Government Accountability Office called for a clearer comprehensive project plan and specific detailed plans for risk mitigation and cost-benefit analyses.[65]

Cargo security is one example of a failure to fulfill requirements in a timely manner. In MTSA, approved at the end of 2002, Congress called on the department in which the Coast Guard would be operating to establish a program to "evaluate and certify secure systems of international intermodal transportation."[66] In January 2004, the task was redelegated (presumably from the Coast Guard) to the Border and Transportation Security Directorate of DHS, which houses Customs and Border Protection. As of June 2005, the program had not been established.[67] Instead, Customs and Border Protection has in effect started implementing it in pieces with C-TPAT, CSI, and other efforts, and is now working with the World Customs Organization on establishing global supply chain standards.[68] It is unclear whether the program has not been implemented because of organizational and capability or capacity issues within DHS or because Congress did not set it as a priority over other programs.

Capacity issues within DHS have been pinpointed as one reason for the failure to implement identification cards as planned. Senior DHS staff members were simply unable to give the program attention because other statutory and security requirements demanded their attention.[69]

---

[65]U.S. Government Accountability Office (2004d), p. 18.

[66]Public Law 107-295, Section 70116. The Coast Guard was in the Department of Transportation, but it was unknown at the time the statute was written which department it would eventually be in when it started implementing MTSA.

[67]Subcommittee on Coast Guard and Maritime Transportation (2005).

[68]Testimony of Robert Jacksta, Executive Director, Border Security and Facilitation, U.S. Customs and Border Protection (Federal News Service, 2005c).

[69]U.S. Government Accountability Office (2004d), p. 9.

The Coast Guard's Integrated Deepwater System program is a final example of lack of implementation. This program was designed to modernize the Coast Guard's sea and air fleet, in light of the Guard's new homeland security duties and the general decrepitude of the fleet.[70] The result of deteriorating ships and aircraft is that the Coast Guard's ability to carry out its missions has been reduced.[71]

Originally designed before the September 11 attacks, Deepwater had to be reformulated afterward to take account of new Coast Guard duties. Unfortunately, by the summer of 2005, the reformulation had not responded to homeland security needs, according to at least some officials providing Congressional oversight.[72] The fault may lie in many places. In part, it may lie in the failure of Coast Guard officials to adequately plan. For example, the Government Accountability Office found that the Coast Guard lacked the type of program management and contract oversight that would lead to a successful outcome. In part, it may also lie in a lack of funding, the responsibility of Congress and the administration.[73] The issue was resolved, for the moment, in July 2005, when the Coast Guard submitted a revised $24 billion plan for Deepwater, to be undertaken between 2002 and 2027. In the Department of Homeland Security Appropriations Act of 2006 (Public Law 109-90), Congress allocated $933.1 million for Deepwater, slightly less than the president's budget request of $966 million.

---

[70]At a U.S. Senate hearing in summer 2005, Coast Guard Commandant Collins said, "Of 41 nations, Senator, that have comparable coast guards or navies, we rank 39th oldest out of 41. The Philippines and Mexico are the only nations that have older fleets" (Federal News Service, 2005a).

[71]U.S. Government Accountability Office (2005d).

[72]Statement of Senator Olympia Snowe (Federal News Service, 2005a); Statement of Representative Martin Olav Sabo (Federal News Service, 2005b).

[73]Reviewing the Coast Guard's Deepwater budget request, Senator Olympia Snowe of Maine said, "It's a number that's driven by the Office of Management and Budget [the White House budget arm] and obviously Congress has contributed to that [lack of resources] with the erratic nature and inconsistent levels of funding year to year" (Federal News Service, 2005a).

Funding

The final major issue in evaluating current U.S. port security programs is funding—specifically, who pays? It was immediately clear with the passage of MTSA that the federal government would not be allocating enough money to cover the costs of MTSA implementation, especially since the section covering port security grants required that federal grants could fund only up to 75 percent of a project rather than the entire project. This became even clearer when the Coast Guard published the interim rule for MTSA on July 1, 2003. Estimated first-year costs of $1.5 billion (Table 7.1) far outweighed estimated appropriations. The Coast Guard and Maritime Transportation Act of 2004 sealed the requirement for non-federal participation with a new report request. Within three months after the law was passed, the secretary of DHS was to report to Congress on funding and was to include a recommendation on "matching requirements to ensure that Federal funds provide an incentive to grantees for the investment of their own funds in the improvements financed in part by Federal funds provided under this program."[74]

The new law also foreshadowed possible solutions to the debate about who pays. Members of the California Congressional delegation have proposed at least three methods alone. These include general fund allocations, a diversion of customs duties, and user fees at the ports. Additional requirements in the new law include making DHS report to Congress estimates of the cost of inspecting vessels in one year, the per-vessel cost, the total cost of inspecting containers in one year, and the per-container costs of these inspections.[75] With these costs in hand, it may be much easier to move to a user-fee system of financing.[76]

---

[74]U.S. Public Law 108-293, Section 804(d)(4). As of early 2006, we could not confirm the status of this report.

[75]U.S. Public Law 108-293, Section 809(b). This report was delivered to Congress in 2005.

[76]Chapter 8 of this volume explores the finance issue in more depth.

Conclusion

The maritime security strategy of the United States includes numerous initiatives—more than those described here—under the broad headings of awareness, prevention, protection, response, and recovery.[77] In some ways, the speed at which programs have been designed and implemented has been remarkable. And there is evidence that they have started to have an effect. Dockworkers, mariners, and the general public are providing more information to the Coast Guard about unusual activity; pilfering and theft within port complexes appears to have fallen, although access control remains a problem.[78] Furthermore, information-sharing mechanisms between the federal government and local stakeholders have been developing, such as through Area Maritime Security Committees and Interagency Operational Centers, among other mechanisms.[79] At the same time, the multiplicity of new tasks has meant that readiness of some Coast Guard tasks has suffered.[80]

What should policymakers do at this point? This chapter has identified four broad areas where policy examination and revision might help. First is the issue of whether policies optimize security programs, resources, and activities. The second is the effectiveness of programs. Third is the problem of unclear authority and priorities. Fourth is the problem of financing. Although presented separately here, they are intertwined in reality—unclear authority may lead to lower effectiveness, for example. Furthermore, a comprehensive cost-benefit analysis, using information on effectiveness that is available only to the government, can help clarify program priorities going forward.

Nearly five years after the attacks of September 11, policymakers should now step back and look at the array of programs and decide whether some should be emphasized or deemphasized. They may find that developing plans and programs to help the maritime system recover from a terrorist incident needs more effort, or that hardening of the ports

---

[77]Hereth and Sloan (2004).

[78]Response of Coast Guard Admiral Craig E. Bone (Federal News Service, 2005c).

[79]U.S. Government Accountability Office (2005e).

[80]U.S. Government Accountability Office (2005f).

as targets should receive more attention. Now that most of the programs have been created and are progressing to some extent, policymakers can also clarify authorities. For example, is the grant program operating under the preferred set of rules? In addition, now that it is apparent which programs are progressing and which are lagging, Congress and the administration can redirect efforts toward those programs they deem most important. No one can claim that such a large and fractious organization as the federal government will respond quickly, but certainly clear direction is better than unclear direction. Finally, funding deserves to be revisited. At a minimum, the government should supply the money necessary to meet its port security goals or mandate actions and payment by private-sector actors (or both) so that these goals are met.

Efforts to reevaluate and coordinate port security are ongoing. In December 2004, the president signed National Security Presidential Directive-41 (NSPD-41)/Homeland Security Presidential Directive-13 (HSPD-13), mandating a National Strategy for Maritime Security. Since then, the Departments of Homeland Security, Defense, and State have led an effort to develop the strategy, completed in September 2005, and eight supporting plans, many made final in October 2005, in consultation with key maritime stakeholders.[81]

Securing the nation's maritime transportation network is clearly important to protecting the nation from terrorist activity. Much has been done. However, without greater conviction on the part of those providing resources and without continued focus on the highest-benefit tasks, the network may remain unnecessarily vulnerable to a terrorist event and unable to respond appropriately should one occur.

---

[81]These eight plans include the *National Plan to Achieve Maritime Domain Awareness*, the *Maritime Transportation System Security Recommendations*, the *Maritime Commerce Security Plan*, the *Maritime Infrastructure Recovery Plan* (undergoing revision in early 2006 to reflect the lessons of hurricanes Katrina, Rita, and Wilma), the *International Outreach and Coordination Strategy to Enhance Maritime Security*, the *Global Maritime Intelligence Integration Plan*, the *Maritime Operational Threat Response Plan*, and the *Domestic Outreach Plan*.

References

"32 Stowaways Found on Ship," *Los Angeles Times,* January 16, 2005.

Adams, Vera, Testimony at a Panel on "Federal Security Structure" hearing on *Security and California Ports*, Office of California State Senator Christine Kehoe, California Office of Homeland Security, and California Association of Port Authorities, Sacramento, California, February 16, 2005.

The Aviation and Transportation Security Act, Public Law 107-71, Washington, D.C., November 19, 2001.

California Department of Fish and Game, Office of Spill Prevention and Response, Legal Unit, *Compendium: The Lempert-Keene-Seastrand Oil Spill Prevention and Response Act and Selected California Statutes Relating to Water Pollution As of January 1, 2003,* Sacramento, California, January 3, 2003.

California Marine and Intermodal Transportation System Advisory Council, Northern California Marine Transportation System Advisory Council, and Southern California Marine Transportation System Advisory Council, *California Marine Transportation System Infrastructure Needs,* Sacramento, California, March 11, 2003.

Chertoff, Michael, "Statement by Secretary of Homeland Security Michael Chertoff before the House Appropriations Homeland Security Sub-Committee," Washington, D.C., March 2, 2005a.

Chertoff, Michael, "Remarks for Secretary Michael Chertoff, U.S. Department of Homeland Security, George Washington University Homeland Security Policy Institute," George Washington University, Washington, D.C., March 16, 2005b.

Coast Guard and Maritime Transportation Act of 2004, Public Law 108-293, Washington, D.C., August 9, 2004.

Crist, Phillipe, *Security in Maritime Transport: Risk Factors and Economic Impact*, Maritime Transport Committee, Directorate for Science, Technology and Industry, Organisation for Economic Cooperation and Development, Paris, July 2003.

Decker, Raymond J., "Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts," Testimony Before the U.S. Senate Committee on Governmental Affairs, GAO-02-208T, U.S. Government Accountability Office, Washington, D.C., October 31, 2001.

Department of Defense and Emergency Supplemental Appropriations for Recovery from and Response to Terrorist Attacks on the United States Act, 2002, Public Law 107-117, Washington, D.C., January 10, 2002.

Department of Homeland Security Appropriations Act, 2006, Public Law 109-90, Washington, D.C., October 18, 2005.

Federal News Service, Inc., "Hearing of the Fisheries and Coast Guard Subcommittee of the Senate Commerce, Science, and Transportation Committee; Subject: The Coast Guard's Revised Deepwater Implementation Plan," Washington, D.C., June 21, 2005a.

Federal News Service, Inc., "Hearing of the Homeland Security Subcommittee of the House Appropriations Committee; Subject: The Coast Guard Deepwater Program," Washington, D.C., June 22, 2005b.

Federal News Service, Inc., "Hearing of the Coast Guard and Maritime Transportation Subcommittee of the House Transportation and Infrastructure Committee; Subject: Implementation of the Maritime Transportation Security Act," Washington, D.C., June 29, 2005c.

Federal Register, *Implementation of National Maritime Security Initiatives, Final Rule,* Table 2. First-Year and 10-Year Present Value Cost and Benefit of the Final Rules, Vol. 68, No. 204, October 22, 2003.

Flanagan, William, "CSI Operations and Overview," presentation to Fifth International Conference on Export Controls, Budapest, Hungary, September 17, 2003.

Flynn, Stephen E., "America the Vulnerable," *Foreign Affairs,* January/February 2002.

Hereth, Larry, "Statement of Rear Admiral Larry Hereth on Maritime Transportation Security Act Implementation Before the Subcommittee on Coast Guard and Maritime Transportation, Committee on Transportation and Infrastructure, U.S. House of Representatives," Department of Homeland Security, U.S. Coast Guard, Washington, D.C., June 9, 2004.

Hereth, Larry, and James F. Sloan, "Statement of Rear Admiral Larry Hereth and Mr. James F. Sloan on the 9/11 Commission Report and Maritime Transportation Security Before the Subcommittee on Coast Guard and Maritime Transportation, Committee on

Transportation and Infrastructure, U.S. House of Representatives," Department of Homeland Security, U.S. Coast Guard, Washington, D.C., August 25, 2004.

Homeland Security Institute, *An Independent Assessment of the Department of Homeland Security's Proposed Strategic Framework for Cargo Security, Homeland Security Cargo Summit, December 16-17, 2004,* Arlington, Virginia, January 28, 2005.

Interagency Commission on Crime and Security in U.S. Seaports, *Report of the Interagency Commission on Crime and Security in U.S. Seaports,* Washington, D.C., Fall 2000.

Loy, Admiral James M., "Luncheon Keynote," Address to Fourth Harbor Safety Committee National Conference, Galveston, Texas, March 4, 2002.

Marine Transportation System Task Force, *An Assessment of the U.S. Marine Transportation System: A Report to Congress,* Washington, D.C., September 1999.

Maritime Transportation Security Act of 2002, Public Law 107-295, Washington, D.C., November 25, 2002.

Office of California Senator Christine Kehoe, the California Office of Homeland Security, and the California Association of Port Authorities, Hearing on *Security and California Ports,* Sacramento, California, February 16, 2005.

Posner, Paul L., "Homeland Security: Reforming Federal Grants to Better Meet Outstanding Needs," Testimony Before the Subcommittee on Terrorism, Technology and Homeland Security, Committee on the Judiciary, U.S. Senate, GAO-03-1146T, U.S. Government Accountability Office, Washington, D.C., September 3, 2003.

Rosen Lum, Rebecca, "Ports Have No Money, But a Wealth of New Security Rules," *Contra Costa (California) Times,* October 28, 2003, Section F, p. 4.

Slater, Eric, "Human Smuggling Operation Probed," *Los Angeles Times,* January 17, 2005.

Subcommittee on Coast Guard and Maritime Transportation, "Hearing on Implementation of the Maritime Transportation Security Act," U.S. House of Representatives, Washington, D.C., June 29, 2005.

Tirschwell, Peter, "A Chat with the Director of C-TPAT," *Journal of Commerce*, January 2, 2006.

"TWIC Awaits TSA Standards," *Journal of Commerce,* Vol. 6, No. 27, July 4, 2005, p. 10.
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) of 2001, Public Law 107-56, Washington, D.C., October 26, 2001.
U.S. Coast Guard, *Port State Control in the United States: Annual Report 2004*, Washington, D.C., 2005a.
U.S. Coast Guard, "List of ISPS/MTSA Major Control Actions," July 19, 2005b, available at www.uscg.mil/hq/g-m/pscweb/detentionSecurity.htm (as of July 26, 2005).
U.S. Coast Guard, "Press Release: Coast Guard Cutter Venturous Changes Command," Office of Public Affairs, U.S. Coast Guard Seventh District, St. Petersburg, Florida, July 14, 2005c.
U.S. Customs and Border Protection, Press Releases about the Container Security Initiative, Washington, D.C., various dates.
U.S. Customs and Border Protection, *Container Security Initiative Fact Sheet,* Washington, D.C., November 1, 2004a.
U.S. Customs and Border Protection, *Global Milestone Reached with 32 Operational CSI Ports,* Washington, D.C., November 12, 2004b.
U.S. Customs and Border Protection, *Fact Sheet: Cargo Container Security—U.S. Customs Border and Protection Reality,* Washington, D.C., October 10, 2004c.
U.S. Department of Homeland Security, Transportation Security Administration, "TSA to Test New ID Card for Transportation Workers," Press Release, August 10, 2004a.
U.S. Department of Homeland Security, *A National Cargo Security Strategy White Paper,* prepared for Homeland Security Cargo Summit, Washington, D.C., December 16–17, 2004b.
U.S. Department of Homeland Security, *National Response Plan,* Washington, D.C., December 2004c.
U.S. Department of Homeland Security, Office of Inspector General, Office of Inspections, Evaluations, and Special Reviews, *Review of the Port Security Grant Program*, OIG-05-10, Washington, D.C., January 2005.
U.S. Department of Transportation, *Port Security: A National Planning Guide,* Washington, D.C., 1997.

U.S. Department of Transportation, *Proceedings of the National Conference on the Marine Transportation System: Waterways, Ports and Their Intermodal Connections,* Airlie Center, Warrenton, Virginia, November 17–19, 1998.

U.S. Government Accountability Office, *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security*, GAO-04-838, Washington, D.C., June 2004a.

U.S. Government Accountability Office, *Maritime Security: Partnering Could Reduce Federal Costs and Facilitate Implementation of Automatic Vessel Identification System,* GAO-04-868, Washington, D.C., July 2004b.

U.S. Government Accountability Office, *Maritime Security: Better Planning Needed to Help Ensure an Effective Port Security Assessment Program,* GAO-04-1062, Washington, D.C., September 2004c.

U.S. Government Accountability Office, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program,* GAO-05-106, Washington, D.C., December 2004d.

U.S. Government Accountability Office, *Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention,* GAO-05-170, Washington, D.C., January 2005a.

U.S. Government Accountability Office, *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security,* GAO-05-404, Washington, D.C., March 2005b.

U.S. Government Accountability Office, *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts,* GAO-05-557, Washington, D.C., April 2005c.

U.S. Government Accountability Office, *Coast Guard: Progress Being Made on Addressing Deepwater Legacy Asset Condition Issues and Program Management, but Acquisition Challenges Remain,* GAO-05-757, Washington, D.C., April 2005d.

U.S. Government Accountability Office, *Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention,* GAO-05-394, Washington, D.C., April 2005e.

U.S. Government Accountability Office, *Coast Guard: Station Readiness Improving, but Resource Challenges and Management Concerns Remain,* GAO-05-161, Washington, D.C., January 2005f.
U.S. House of Representatives, *House Report 109-079—Department of Homeland Security Appropriations Bill, 2006,* Washington, D.C., May 13, 2005.
U.S. Office of Management and Budget, "Department of Homeland Security," in the President's 2005 Budget, Washington, D.C., February 2, 2004.
U.S. Office of Management and Budget, *Draft 2005 Report to Congress on the Costs and Benefits of Federal Regulations,* Washington, D.C., 2005.
Willis, Henry H., and Davis S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain*, the RAND Corporation, TR-214-RC, Santa Monica, California, 2004.
Wrightson, Margaret T., "Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges," Testimony Before the Committee on Commerce, Science, and Transportation, U.S. Senate, GAO-05-448T, U.S. Government Accountability Office, Washington, D.C., May 17, 2005a.

8. Financing Port Security

Jon D. Haveman and Howard J. Shatz
Public Policy Institute of California

Introduction

The federal government has used a variety of policy instruments in its efforts to protect the ports and secure the supply chain for traded goods shipped by sea. These include direct provision of services by the federal government and indirect provision through new laws and regulations covering private and public actors, such as ports and trade intermediaries, all along the supply chain.

A number of new measures increase costs for all actors. These include the development and implementation of security plans for ports and ships, new infrastructure investments, increased local government training and staffing for response and recovery, actions by shippers to secure their supply chains, and increased staffing, training, and equipment for federal agencies such as the U.S. Coast Guard. Currently, the U.S. government is appropriating money out of its general funds for increased port security. Private businesses and ports are bearing costs through their compliance with regulations or through actions responding to incentives established by the government programs. Security improvements at ports also receive modest funding from federal grants, as described in Chapter 7 of this volume.

These new measures, and their cost estimates, have raised one of the knottiest problems in the area of homeland security. Specifically, who should pay for implementation, and how should the money be raised? In this chapter, we concern ourselves with these questions. We do not address the issue of whether these new measures represent an optimal use of available policy instruments; this is addressed elsewhere in this volume. Furthermore, our discussion emphasizes questions of economic efficiency rather than political feasibility or issues of equity.

Securing the nation's ports involves the consideration of two distinct threats. The first is an attack directed at disrupting activities in the port itself. The second is the use of the port as a conduit through which terrorists can transport materiel for use anywhere in the country.

The principal statute detailing measures to protect ports is the Maritime Transportation Security Act of 2002 (MTSA), which specifies extensive prevention, response, and recovery planning. The U.S. Coast Guard is largely responsible for overseeing implementation of MTSA measures and has prepared the implementing regulations and developed a cost estimate of compliance. In total, the Coast Guard has estimated a 10-year implementation cost of $7.3 billion without any elevated security conditions.[1]

The key programs in keeping ports from becoming conduits through which terrorist materiel could enter the country are the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT). The very existence of the CSI reflects the reality that a large proportion of waterborne trade now moves in ocean shipping containers, which can hold almost anything, including weapons and people. The CSI program places U.S. customs officials at foreign ports, aims to inspect high-risk containers at foreign ports before those containers leave for the United States, and facilitates the adoption of more secure containers. C-TPAT encourages private businesses to develop plans and take steps to increase the security of their supply chains, from the original manufacturer to arrival at the U.S. port. One cost analysis of various port security measures declined to estimate the cost of improvements in the container system under the CSI, but suggested that the potential costs of C-TPAT "are great, as [participants] must invest in securing the physical integrity of their own premises, but also ensure that their trading partners do so as well."[2]

Because improving security requires extra spending, and because no extra revenues for this spending are apparent, financing is an important issue. To examine funding alternatives and shed light on efficient financing, we turn first to the study of public finance within the

---

[1]Federal Register (2003).

[2]Crist (2003), p. 53 (CSI) and p. 54 (C-TPAT).

economics discipline. This field provides a well-developed background for understanding whether public resources should be devoted to the issue, the economically efficient allocation of financial responsibility between the private and public sector, and sensible approaches to raising the money.

The strongest justification for government participation in finance or for government regulation, both a form of collective action, is the presence of a market failure. This is a situation in which private markets fail to provide an optimal amount of a desired good or service or the market participants do not capture all costs or benefits. We provide a discussion of market failures that may be present with respect to the provision of port security and discuss some well-known policy examples and their funding mechanisms to tease out lessons for the economically efficient financing of port security.

The first market failure is found in the public goods aspect of port security: Because everybody in society benefits from port security, there is very little incentive for private industry to provide as much as is efficient. A second market failure is that of a negative externality: Engaging in waterborne international trade creates a mechanism for transporting terrorist materiel, endangering others in society. A final market failure is the weakness of private insurance markets for the ports. Ideally, insurers would spread the risk of an attack across all 361 seaports in the United States, in much the same way that they do with automobile and homeowners' insurance.[3] Although insurance coverage is currently available, it is not clear how many participants in the maritime transportation industry have taken it up, and it is not clear whether such insurance covers the likely terrorism threats.

Our research leads us to conclude that there is an efficient sharing of the burden of paying for port security measures between the public and private sectors. Although we are unable to determine a precise division of the funding responsibility, our analysis suggests that both the public and private sectors should play a significant role in providing financing.

---

[3]Although there is no specific seaport terrorism insurance, there is more general terrorism insurance written under commercial property and casualty lines.

With these public finance principles as a backdrop, we discuss a number of current proposals for port financing. In the end, we find that the current approach is likely appropriate, although the relative contributions of public and private sectors may require some adjustment. Compliance with costly regulation is an efficient way to elicit financial contributions from the private sector for port security. In the event that the private sector's optimal contribution to port security should exceed that accounted for by current regulations, then new mechanisms should be used to draw additional money from business. In this case, taxes on port activity or on the goods movement industry may be necessary to offset government expenditures on port-related activities. The converse is also true: The optimal financing of port security may, in the end, require a transfer from general government revenues to the ports. We also find a role for government participation in terrorism insurance markets. In particular, with respect to insuring the ports, there is scope for government support of the private insurance market and for some subsidization of insurance premiums by the federal government.

Efficiently Financing Port Security

Public policies are enacted for a wide variety of reasons, including both equity and efficiency considerations. The development of economically efficient public policies relies on applying two fundamental principles: The beneficiary of the policy should pay for it and the price of an activity should reflect all costs involved. Identifying these beneficiaries then structuring a system of fees and payments accordingly are key to the efficient financing of port security.

The dual security threat—to ports themselves and to the country as a whole through the ports—makes port security susceptible to elements of three market failures, which in turn suggests a role for government financing or regulation. These market failures include the provision of a public good, national security; a negative externality, the danger introduced to the rest of the country by maritime activities; and the absence of a market through which the ports could insure against terrorism related damages.

Public Goods and Port Security

The ports' position as a dual threat represents a vulnerability in the nation's defense system, one different from those addressed by traditional forms of national defense; the means by which this vulnerability is eliminated also differ. Nonetheless, the prescription for an efficient payment system, for port security in this case, is the same as for national defense. All citizens benefit; therefore, general government revenues are an appropriate source of funding.

This prescription for funding is derived from the identification of national defense as a "public good." Public goods are characterized as non-exclusive and non-rivalrous. They are non-exclusive in that providing the service to one person includes providing the service to others. They are non-rivalrous in that the benefits received by one person from their provision do not detract from the benefits received by another. Public goods are underprovided or inefficiently provided by private markets and are therefore good candidates for government activity. This is particularly evident with national defense, which likely would not be available without a formal government program.

The need to protect society from the physical threat of dangerous materiel flowing through the ports and the broader waterborne supply chain is the source of the public goods nature of port security. Terrorism entails an additional threat that is not present with the provision of most public goods. That is, whether a port or some other location is struck, a terrorist attack has costs well above and beyond the economic. As Stephen S. Cohen discusses in Chapter 4 of this volume, there is a real danger of an extreme emotional response by the general public to a terrorist attack. Likening this response to the human body's autoimmune defenses, he points out that there is the danger of "reactions on our part that are themselves vastly more damaging than the initial terrorist act." This additional cost strengthens the case for preventing terrorism and its effects and hence strengthens the case for government provision of this public good.

Negative Externalities and Port Activity

The second market failure arises from the negative externality placed on society by the international movement of goods by shippers, ocean

carriers, and port and terminal operators. The goods movement infrastructure itself provides the means by which terrorists can move their weapons, thus endangering all of society beyond a port's gates. In essence, the movement of goods internationally by water imposes a cost on the rest of society that is not reflected in the price of these services.

Externalities arise when an activity undertaken by one individual affects the welfare of another either positively or negatively. In the case of power plants or industrial production, pollution is a negative externality, the cost of which is not paid for by anyone, except in the form of health effects, for example, that are borne by people who do not necessarily consume the product or service. Where an activity results in a negative externality, more of that activity occurs than is economically efficient. When making the decision to produce electricity, the company takes into account only its private costs. When making the decision to purchase electricity, the consumer decides on the basis of the price charged. Were pollution costs incorporated into production and consumption decisions, less power would be consumed and therefore less would be produced.

Government intervention is often employed to address externalities. In the abstract, a tax is the prescription for addressing a negative externality. The tax causes producers to internalize, or take account of, this additional cost when making production and pricing decisions. Conversely, with a positive externality, a subsidy is appropriate. This again causes the producer to internalize the externality and take the benefits into consideration in pricing and production.

In specific instances, however, a direct tax or a subsidy may not be the most efficient policy for addressing an externality. Instead, some form of regulation may be appropriate. In the particular case of pollution, a variety of regulatory mechanisms have been applied. In particular, with regard to pollution from automobiles, the preferred mechanism has been fuel efficiency standards. With regard to electricity production, some form of pollution permitting system may prove to be more appropriate. In either case, the cost of reducing the externality is largely born by the polluter.

Similarly, the costs of any mechanism designed to reduce the security burden resulting from activity at the ports ought to be borne by those

benefiting from this activity. Identifying those benefiting is no easy task. Certainly, those involved in providing goods movement services benefit, as do the companies (both domestic and foreign) that buy and sell the traded goods and even customers who purchase foreign goods that might be cheaper, better, or different from those produced in the United States.

That the benefits of international trade permeate society is not necessarily a call for further government support of security measures. As the benefits of international goods movement spread beyond those directly participating in the activity, so too do the costs of implementing greater security measures. Because costs such as taxes or compliance with regulations can often be partially passed through to customers or suppliers, the ultimate payer often differs from the person or business responsible for the payment. Imposing costs on waterborne goods movement, therefore, results in all those who benefit bearing some share of the burden.

Whether a tax or some form of regulation is appropriate for addressing the maritime goods movement externality depends on the reason for the externality. The volume of containers is enormous, but it is not the volume, per se, that is responsible for the externality. Although it is true that it would be easier to hide something in one container among 10 million than in one container among 10, reducing the volume by 10 percent or even 20 percent would not likely reduce the potential for smuggling contraband into the country. What would reduce the risk is changing the way that the flow of containers is handled and protected, or securing, or sealing, the system. It is the system that is responsible for the bulk of the externality. As it is not clear how a tax on the security of the system would be implemented, direct regulation of the security with which containers are handled is likely to be more appropriate. This could involve mandating inspections, container seals, and other similar security measures at various points along the supply chain.[4]

As with a tax, the financial burden of mandatory security measures will be distributed throughout the supply chain, with broader society also bearing the burden in the form of higher prices for imported products.

---

[4]See Chapters 4 and 5 of this volume for more on these measures.

Regulation, therefore, is consistent with the principle stated earlier that the costs of reducing the externality ought to be borne by those benefiting from the activity.

Regulation is also more consistent with the efficient use of maritime resources. Although a tax would impose a cost burden on each individual container, complying with many security regulations imposes a cost that is to some extent independent of the number of containers processed.[5] Therefore, regulation is less likely to divert the flow of containers to other transportation modes such as air or to ports in other countries and subsequent land transport to the United States. These tax-related distortions lead to a less-efficient use of resources than would occur under regulation. Raising the funds for compliance would be at the discretion of the industry. However, it is likely that they would be extracted lump sum out of profits or perhaps capital expenditures rather than out of revenues raised on a per-container basis.

Regulation, or even the threat of regulation, may have one other effect. Faced with the possibility of more rules, the private goods movement industry might innovate security solutions on its own to forestall more government action. This "stick" approach could be complementary to the more "carrot"-like approach described by Jay Stowsky in Chapter 5 of this volume.

In our examples of national defense and pollution, identifying the responsibility for paying for programs was clear. For port security, however, the question turns on whether port security is a public good or whether the risks caused by maritime trade are negative externalities. The externality is clear: But for waterborne goods movement, this particular vulnerability of society to terrorism would not exist. However, but for geopolitical issues that are unrelated to waterborne goods movement, there would be no such externality and no such risk of terrorism as currently exists. These observations leave us unable to pin the risk of maritime terrorism on only one or another of these two market failures alone. This suggests that a sharing of the burden between

---

[5]In particular, the development and implementation of port security plans. Fences and armed guards at the ports or immensely expensive container scanning equipment also represent fixed costs rather than distorting marginal costs such as a container tax.

society—through government-provided financing—and the private sector is appropriate.

Creating a formula for the appropriate allocation of the financial burden is highly complex, involving calculations of society's overall gains from trade and the share of those gains in the waterborne goods movement industry. Turning that formula into policy also requires considerations of political feasibility, social equity, and ideological, political, and bureaucratic forces. The quantification of gains is beyond the scope of this chapter, and judgments about equity are for policymakers. The quantification is further complicated by the third market failure associated with the need for port security—the absence of appropriate insurance markets.

The Absence of Private Insurance Markets

Although much of the emphasis of port security focuses on protection from terrorist acts, the reduction of harm suffered in the event of an attack is also important to protecting society from terrorism.[6] Policies to prevent or ameliorate the effects of terrorism at a port are analogous to policies to reduce harm from natural disasters such as floods, earthquakes, and hurricanes.

The need for terrorism insurance arises from the fact that, at any point in time, it is unlikely that a given seaport will possess the resources with which to rebuild or recover after a terrorist attack. Some spreading of this financial risk across all ports, all potential terrorism targets, or broader society is necessary to assure the resumption of economic activity supported by the functioning of the ports. Yet, there is only a limited insurance market to provide this function. The deficiency of such a market is a third market failure and suggests an additional role for government policy.

In the wake of massive insurance losses from the September 11 attacks, the insurance industry and federal policymakers were concerned that the insurance market for terrorism risk would disappear. The value

---

[6]The White House (2002) defines homeland security as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and *recover from attacks that do occur*" (emphasis added). See Chapter 6 of this volume for more on recovery following a terrorist attack.

of such insurance is that it can help businesses—ports, in this case—sustain operations during a disruption and rebuild quickly, blunting the effects of a terrorist attack.[7] Responding to these concerns, the U.S. Terrorism Risk Insurance Act of 2002 (TRIA) provided for federal reinsurance, or insurance for the insurance companies, at no cost. It explicitly applied to ocean marine vessels and their cargo, business interruption insurance applicable to the ocean marine industry, and marine-related liabilities,[8] and likely applied to the commercial property and casualty insurance held by terminal operators at the ports. The act was temporary but was extended through December 31, 2007, by the Terrorism Risk Insurance Extension Act in December 2005. Despite the backstop, the original act did not provide for and the extension does not require coverage for chemical, biological, radiological, or nuclear terrorism. As a result, there is little insurance available for these risks, and these are the very risks that are among the greatest concerns to the maritime industry.

The private provision of insurance for events similar to a terrorist attack has been tried and found unprofitable in the past.[9] There are five factors working against the success of these efforts: adverse selection, moral hazard, inaccurate risk forecasting, the lumpiness[10] of the events, and the undervaluation of insurance by potential victims. Adverse selection results from the likelihood that only those most at risk of a flood, earthquake, or terrorist attack will purchase the insurance. Therefore, the private providers of such insurance will have difficulty spreading the risk sufficiently so that the premiums are affordable. The moral hazard arguments suggest that, having purchased the insurance, individuals will invest too little in other protection or will locate in areas that are subject to even greater risk than otherwise would have been the case.

---

[7]Chalk et al. (2005).

[8]U.S. Department of the Treasury (2005),

[9]In particular, private markets have failed in their attempts to provide flood insurance. As a result of this failure, the National Flood Insurance Act of 1968 was put in place. This program makes flood insurance available where it otherwise would not be.

[10]By lumpiness, we mean that they occur infrequently and affect a large group of individuals or structures.

The inability to accurately forecast the risk of a terrorist attack is another contributing factor in preventing the profitable functioning of this insurance market.[11] The insurance industry has gotten better at estimating what its losses might be from a terrorist event, but estimating the probability of such an event remains extremely murky.[12] In their desire to insulate themselves from inaccurate forecasts of risk, private insurance companies will likely overprice coverage, leading to lower take-up rates.

That terrorist events are lumpy further adds to the difficulty in profiting from this type of insurance provision. Private insurance generally functions well when there is independence of risk among the insured. Consider one million homes, each of which faces some small probability of a house fire that would create a large loss. For insurance against that loss, each homeowner would gladly pay a premium equal to the expected value of that loss, meaning the value adjusted for the probability of the event. If the probability that one house catches fire is independent of the probability that any other catches fire, an insurance company can offer each a policy with that premium and have a very certain income stream. This independence of risk means that the percentage of houses catching fire during any period will always be very close to the probability that any one house catches fire. The insurance company can pool risk and turn individual risk into near aggregate certainty.

This pooling does not work with one-time events such as terrorist attacks or natural disasters. The probability that one insured entity is damaged through terrorism is small, but it is not independent of the probability that other insured entities will also be damaged. Therefore, in a given year, the percentage of a company's insured houses being damaged by terrorism will never be close to the probability that any one insured house is damaged. The probability that any one house is damaged is equal to the probability of an attack, whereas the percentage of a company's insured homes damaged in the event of an attack will be

---

[11]See Jaffee and Russell (1997) on uninsurable risks and Kunreuther (2002) for a detailed analysis of such risks, with particular attention to terrorism.

[12]U.S. Department of the Treasury (2005).

either zero or some number much higher than the probability of an attack. So, pooling risks leaves the insurance company facing significant variability in payouts and great uncertainty in its income stream. Providing this insurance is therefore a very risky proposition.

A final problem, and one that is particularly important with respect to the ports and other forms of infrastructure, is the undervaluation of insurance on the part of potential victims.[13] Generally, this problem derives from a lack of perceived vulnerability, which leads to an unwillingness by potential victims to pay for even actuarially fair insurance. In the case of ports, this problem is magnified by their contribution to the functioning of the broader economy. Ports are part of large transportation networks. A disaster at a port will certainly cost that port, but it will also cost all users of the port, with potentially large ripple effects throughout the economy. Without some type of incentive, ports may not take these ripple effects into account and will underinsure.

Where private markets fail, governments can intervene. Perhaps the easiest form of intervention would be in the public provision of insurance, with a mandate that all at-risk entities maintain coverage. Where government can efficiently intervene in the case of natural disasters and terrorism is in providing access to actuarially fair premiums for likely victims of such one-time events.[14] Governments have the resources available to bear the risk of a bad outcome, whereas a private insurance company likely does not; as well, it has a responsibility to its shareholders to avoid risk it cannot financially support. Providing actuarially fair premiums that reflect security measures at the ports will provide incentives for the investment in better security by the ports, terminal operators, and those along the supply chain.

A number of arguments are in favor of government participation in terrorism insurance markets, if not direct provision. These include the potential of widespread economic disruptions from terrorism, the ability

---

[13]This is well documented with respect to natural disaster insurance. See Palm (1995) for evidence of take-up rates for earthquake insurance.

[14]Actually determining what an actuarially fair premium is for likely policyholders is another element of risk. Our experience with terrorism is not sufficient to provide evidence for who is at just how much risk and hence the probability that any individual will be injured.

of government to achieve greater diversification than private companies, and the fact that governments can have a large influence on terrorism risk through their counterterrorism, defense, and foreign policies. However, government participation also carries problems, including the potential crowding-out of private insurers, inefficient bureaucracy, and a stifling of entrepreneurial solutions.

An alternative to directly providing such insurance is for the government to provide reinsurance, in effect insuring the insurance companies. In this way, the companies can take on risk from those under threat of terrorism (the ports) and pass on a portion of that risk to an entity (the federal government) that can afford the potential very large payout a massive, successful terrorist attack would cause.[15] The aforementioned TRIA is just such a policy.

Neither direct provision nor reinsurance alone solves all the problems related to the demand for insurance. In particular, the likelihood remains that agents in the maritime industries will underinsure, so too do the issues of adverse selection and moral hazard. Some form of regulation or subsidization of premiums is therefore also likely necessary. Regulation in the form of mandatory insurance, or the appropriate sealing of the supply chain, would help alleviate adverse selection and moral hazard, respectively. Subsidizing premiums to the point where take-up rates are high enough is another option, although deciding what rates are high enough is a complicated proposition.

Methods for Financing Port Security

As yet, no strategy for financing port security has been clearly articulated. However, one is taking shape involving a mixture of government funding and regulations. The regulations are imposed on those in the waterborne goods movement industry, including shippers,

---

[15]Numerous governments provide variations of either insurance or reinsurance coverage (Organisation for Economic Cooperation and Development, 2005). Even before 2001, the governments of Israel, South Africa, Spain, and the United Kingdom backed up private insurers in one form or another. For example, in the United Kingdom, a mutual insurance company known as Pool Re provides reinsurance for which the government is by agreement the lender of last resort should Pool Re exhaust its capital. France also acts as a reinsurer of last resort for terrorism risk there, as of January 2002. In contrast, Austrian insurance companies created a private co-reinsurance pool in 2002.

carriers, terminal operators, and port authorities. The government is funding port security measures through grants to the industry and public agencies and greater resources for personnel, equipment, and programs for federal departments with purview over port security.[16]

In all, the federal government has contributed a relatively small share of the overall expenses associated with port security. Perhaps as a consequence, some state governments are getting involved in providing a funding source. In California, legislators introduced bills in both the state Senate and Assembly to generate a revenue source for ports to draw on in providing security.[17] Each measure included a $10 fee per each twenty-foot-equivalent unit (TEU) of containers that would have been devoted to securing the ports.[18] However, the senate bill has not yet passed, and the assembly bill was amended to include only a study of port security financing and did not institute a fee. Even so, it was vetoed by the governor. A bill still working its way through the legislature includes a bond issue to allocate $100 million for port security grants.[19]

Given the justification for government financing outlined in the previous section, where should the government money come from? In the years since September 11, various members of Congress have proposed legislation for their preferred method of financing port security. As of the end of 2005, three proposals had emerged from

---

[16]In addition to the programs discussed in Chapter 7 of this volume, support for U.S. Coast Guard activities has increased by more than $2.5 billion, from $4.95 billion in fiscal year 2001 to almost $7.58 billion in fiscal year 2005 (U.S. Coast Guard, 2003, 2004, and 2005; U.S. Department of Transportation, 2002).

[17]California State Assembly Bill 1406, "Ports and Harbors: Freight Security Fee," introduced by Assembly Member Betty Karnette on February 22, 2005, and California State Senate Bill 760, "Ports: Congestion Relief: Security Enhancement; Environmental Mitigation: User Fee," introduced by Senator Alan Lowenthal on February 22, 2005. AB 1406 was passed by the Legislature and vetoed by Governor Arnold Schwarzenegger. SB 760 was awaiting consideration in the California Assembly as of April 2006.

[18]Containers are generally 40 feet long. However, a common measure of container volumes is the twenty-foot-equivalent unit, or TEU. A 40-foot container is two TEUs.

[19]California State Senate Bill 1024 was introduced as the "Essential Facilities Seismic Retrofit Bond Act" by Senate pro Tempore Don Perata and Senator Tom Torlakson on February 22, 2005. It has since been amended to the "Safe Facilities, Improved Mobility, and Clean Air Bond Act." Governor Arnold Schwarzenegger has made similar proposals in an infrastructure bond plan. As of April 2006, no action had been taken on infrastructure investment or security spending for California ports.

within the California Congressional delegation alone, and these capture much of the debate within the port community.[20] Representative Juanita Millender-McDonald has proposed that the U.S. government allocate $800 million each year for five years from general funds for port security. Representative Dana Rohrabacher has suggested that port authorities be allowed to levy user fees on containers to raise money to pay for security improvements. And former Representative Doug Ose has proposed that part of U.S. customs duties be diverted to pay for port security. This last proposal has gained the support of California port officials, who appear to want these duties to be allocated on the basis of where they are collected.[21]

A fourth option, a national user fee on cargo and passengers, was discussed during the U.S. House-Senate conference on MTSA, but this was not included in the legislation.[22] The requirement for a mandatory fee was reintroduced in 2004, but again did not meet Congressional approval.[23] Others have backed the idea that ports levy their own fees or special assessments to pay for security improvements. These suggestions have been accompanied by requests for additional federal funding or by suggestions that the federal government should play no role in security improvements within a port.[24]

---

[20]These are HR 3712 (2004), the "United States Seaport Multiyear Security Enhancement Act," proposed by Representative Juanita Millender-McDonald; HR 3028 (2003) and HR 494 (2005), an amendment to the Water Resources Development Act of 1986 to expand the authority of non-federal interests to levy harbor fees, proposed by Representative Dana Rohrabacher; and HR 2193, the "Port Security Improvements Act of 2003," proposed by Representative Doug Ose and Representative John Tierney (of Massachusetts). A new bill, the "Security and Accountability For Every Port Act," or "SAFE Port Act," HR 4954, introduced by Representatives Dan Lungren and Jane Harman on March 14, 2006, proposes allocating $400 million per year out of customs duties for six years for port security grants, and $401 million per year, with the source not identified, for six years for other port security programs.

[21]This view emerged in testimony at a hearing entitled *Security and California Ports*, sponsored by the Office of California State Senator Christine Kehoe, the California Office of Homeland Security, and the California Association of Port Authorities and held in Sacramento, California, February 16, 2005.

[22]Senator Ernest F. Hollings of South Carolina pushed for this (Frittelli, 2003).

[23]S. 2279, introduced by Hollings and Senators John McCain and John B. Breaux.

[24]Godwin (2003); Lanier (2003).

Benefits and Costs

There are benefits and costs to all of these methods of financing. An allocation from general funds would be administratively simple and could be large enough to pay for all desired improvements. However, it would also mean that other programs would have to be cut. In addition, as a matter of economic efficiency, the goods movement industry, which is a prime beneficiary of maritime transportation infrastructure, ought to shoulder at least a portion of the cost directly.

A diversion of customs duties would also be administratively simple, qualitatively similar to using general revenues, and would not be unprecedented. Thirty percent of customs duties are already earmarked for agricultural and food programs, and other duties are diverted to migratory bird conservation, sports fish and aquatic resources, and reforestation.[25]

There are three arguments against the use of customs duties, however. First, the undedicated (70%) portion of these duties is already used to pay for other programs, so diverting them will mean cutting those programs. There is no clear indication that the particular programs currently funded by tariff revenue are any better candidates for cutting than are programs not funded by tariff revenues.

Second, advocates sometimes discuss duties collected at ports as something generated by ports.[26] However, duties are not related to the use of the transportation system. Rather, they are taxes on imports imposed without regard to the mode of transportation.[27] Shippers use seaports not because they get a better deal on tariffs there, but because in some cases it is cheaper or more convenient to use ocean transport than air transport (from anywhere in the world) or land transport (from Canada or Mexico). The claim made by seaports as to their entitlement

---

[25]U.S. Government Accountability Office (2002).

[26]See, for example, Godwin (2003), and testimony at a hearing entitled *Security and California Ports*, sponsored by the Office of California State Senator Christine Kehoe, the California Office of Homeland Security, and the California Association of Port Authorities and held in Sacramento, California, February 16, 2005.

[27]U.S. Government Accountability Office (2002).

to the collected duties is comparable to that of a large local retailer staking a claim on the sales tax revenue that it generates.

Third, diverting duties will create a constituency that wants to retain duties, a position counter to long-term U.S. trade philosophy. The United States has aggressively sought to lower worldwide tariffs since even before World War II, and most recently took the lead on starting a new round of trade liberalization negotiations, the World Trade Organization's Doha Development Round. Creating a powerful group that benefits directly from tariffs—ports, terminal operators, and other goods movement industry participants—would run counter to six decades of U.S. trade policy.

A national container or cargo fee with revenues earmarked for security could provide a larger and more stable source of funds for security than would a budget allocation.[28] It would also place the burden on the entity that actually used the ports for transportation purposes. Depending on market structure, this fee could get absorbed by the importing company, could get passed through to the final consumer, or could get passed back up the shipping chain to the foreign manufacturer.[29]

There are two particular objections to this idea, however. First, such a fee could cause shippers to divert some of their cargo to airports or to Canadian or Mexican seaports—such as Vancouver and Halifax in Canada and Manzanillo and Veracruz in Mexico—from where they could be transported by truck into the United States. Second, such fees might violate international trade agreements to which the United States is a party.[30]

---

[28]The maritime industry will certainly take exception to the notion that it would provide a stable source of funding. This sense results from their experience with the Harbor Maintenance Fee, which annually adds to the Harbor Mainenance Trust Fund. In 2002, the fund had a balance of $1.9 billion, an amount equal to approximately 2.5 years worth of revenue from the Harbor Maintenance Fee. This fee is designed to help fund maritime infrastructure improvements. With ample demand for dredging, wharf repair, and the like, industry representatives wonder why these funds are not being disbursed.

[29]This latter option is the one envisioned by Rohrabacher (2003) in his testimony on local container fees.

[30]Lanier (2003).

As container fees would put U.S. seaports at a disadvantage relative to other modes or ports in other countries, they could result in an inefficient allocation of resources. If this diversion were to reduce the threat or vulnerability from terrorism, it might well be appropriate. However, because we have identified the problem as the process of moving goods rather than the volume of goods moved, our earlier discussion indicates the desirability of some regulation of goods movement practices that would likely result in a smaller reduction in volumes and, hence, less inefficient diversion.

We do not address the implications of international agreements for container fees. Although potentially very important, this issue falls within the realm of international politics. It would involve uncertainties about whether any other country would challenge such fees and whether the United States could successfully negotiate the ability to use such fees if there was an unsettled question under international law.

Two additional considerations are worth discussing here. The post-September 11 regulation of security is already imposing a substantial financial burden on the goods movement industry. As we indicated in the discussion of economic efficiency, society at large receives substantial benefits from increased security at America's ports. If user fees are used to offset the contribution derived from general revenues, an inefficient burden could be placed on the ports. In particular, were user fees ultimately to be the only source of government funding for port security, the burden that is rightly imposed on broader society now falls back on the goods movement industry and its beneficiaries.[31]

Another consideration has to do with equity within the waterborne international shipping community. In particular, the Coast Guard has estimated that a disproportionate share of the security costs over time will be borne by oil terminals. Generating revenue for port security through a container fee or some other general cargo or passenger fee

---

[31]Approximately 10 million containers arrive at U.S. ports each year. The U.S. Coast Guard estimates a 10-year cost of $7.3 billion for MTSA implementation, assuming no episodes of elevated security states, and this would imply a container fee of $73 per container. Accounting for elevated security episodes, the container fee would likely have to be more than $100 per container. Research is not available that would indicate the extent to which a fee of this magnitude would generate pressure to divert.

suggests that security at oil terminals would be subsidized, since these terminals would not be subject to such a fee. In addition, oil terminals may not receive appropriate attention and resources if the revenues are disproportionately the result of container traffic. Each of these issues should be carefully considered when evaluating alternative revenue sources.

A local user fee will have many of the benefits and costs of a national user fee, but with one additional problem. Ports within the United States compete fiercely with each other. Any single port may be reluctant to institute a fee if its competitor ports do not institute the fee, because the fee-charging port will then be more expensive to shippers. It may also become more secure, which could attract business, but the balance of these two effects is uncertain.

Given the justifications for federal financing, and the problems associated with tariff diversion and user fees, dedicating a specific amount from general revenues appears to be both the most administratively simple and least inefficient method of providing financing. However, given the justifications for private financing, it is not necessary that whatever federal amount emerges cover the entire cost of improving port security. Efficiency arguments based on public finance principles suggest that users and beneficiaries of the system should directly pay some share of the costs, and compliance with broad regulations appears to be the most efficient means of spurring their contribution, although perhaps not the only means necessary.

Implications for Financing Port Security

The discussion of public goods, externalities, and insurance in this chapter sheds light on the appropriateness of government involvement in financing port security and suggests steps that government should consider. In particular:

- The national defense nature of port security suggests that government contributions are justified. Society as a whole will be protected, and private voluntary actions will not provide the optimal amount of protection.

- The negative externalities generated by the maritime supply chain suggest, however, that the private actors that gain from the maritime goods movement infrastructure should also provide financing, internalizing the costs.
- Finally, a government-mediated risk-spreading strategy, such as assistance to create an active terrorism risk insurance market, might provide incentives for private actors to take preventive actions.

The market failures inherent in the private provision of port security suggest that there is an optimal sharing of the burden between government and private actors. Unfortunately, we are not in a position to identify specific shares. Such identification requires an evaluation of the relative likelihoods of the use of a port as a conduit versus a target. It also requires the inclusion of equity considerations, which can be derived only from the political process.

Rather than propose an optimal split, we have presented key factors for policymakers to consider. Our discussion indicates that there are substantial differences in the relative merits of current proposals for government financing of port security. In particular, the economic arguments presented throughout suggest the appropriateness of general government revenues over user fees or the specific revenue stream derived from import tariffs. Although user fees do have the desirable feature of imposing the burden on the goods movement industry, they do not spread the burden across broader society as is indicated for economic efficiency. User fees serve to increase the burden on the goods movement industry beyond that already imposed by government regulation. This is perhaps a justifiable outcome, but the observation is important in the consideration of user fees versus general revenues as a funding source. In particular, user fees alone do not constitute an efficient funding of port security measures and are arguably not the best way to secure private contributions. As discussed above, it is not clear that the results of a tax on waterborne goods movement, whether these are simply reductions of imported goods volume or diversion to other modes of transportation, is efficient. Costly compliance with federal regulations may be more appropriate.

The current burden of financing port security falls along the following lines. The federal government has assumed the responsibility of paying for government services. These include services provided by the U.S. Coast Guard, Customs and Border Protection, and other agencies, such as patrolling local waters, monitoring compliance with a variety of regulations, and staffing the Container Security Initiative and other programs. Private entities in the goods movement sector are broadly responsible for the rest, including the implementation of MTSA provisions and the voluntary compliance with C-TPAT membership, although grants from the federal government help defray a small portion of the MTSA implementation costs. State and local governments are also contributing funds in the way of grants directly to ports for implementing port security measures. This division of the burden of financing port security is surely convenient, but the issue of its economic efficiency is one that is yet to be determined. It is surely most efficient for the goods movement industry to finance compliance with regulations and the government to finance government services. However, it is entirely possible that the optimal financing split will involve the private sector paying for the provision of government security services or the government subsidizing the provision of private security services.

Increasingly, the burden of paying for port security and security along the supply chain is being borne by participants in the waterborne goods movement industry. This is happening in part because over time, costs of personnel and operation and maintenance of security equipment will grow as a proportion of security spending. To date, federal and state grants have not been available to defray these costs. On economic efficiency grounds, there may be scope for public participation in the financing of port security in a greater amount than is now being spent. Although economic efficiency suggests a substantial sharing of the burden, the relative burdens will ultimately be determined by the political process, which considers economic efficiency as only one of many factors.

References

Chalk, Peter, Bruce Hoffman, Robert T. Reville, and Anna-Britt Kasupski, *Trends in Terrorism: Threats to the United States and the*

Future of the Terrorism Risk Insurance Act, the RAND Corporation, MG-393-CTRMP, Santa Monica, California, 2005.

Crist, Phillipe, *Security in Maritime Transport: Risk Factors and Economic Impact*, Maritime Transport Committee, Directorate for Science, Technology and Industry, Organisation for Economic Cooperation and Development, Paris, July 2003.

"Essential Facilities Seismic Retrofit Bond Act," California State Senate Bill 1024, Introduced by Senate pro Tempore Don Perata and Senator Tom Torlakson, Sacramento, California, February 22, 2005.

Federal Register, "Implementation of National Maritime Security Initiatives, Final Rule, Table 2. First-Year and 10-Year Present Value Cost and Benefit of the Final Rules," Vol. 68, No. 204, October 22, 2003, p. 60467.

Frittelli, John F., *Maritime Security: Overview of Issues,* CRS Report for Congress, Congressional Research Service, Library of Congress, Washington, D.C., February 24, 2003.

Godwin, Jean C., "Testimony of Jean C. Godwin, Executive Vice President and General Counsel, American Association of Port Authorities, Hearing on Financing Port Infrastructure, Before the House Transportation and Infrastructure Subcommittee on Water Resources and the Environment," Washington, D.C., November 20, 2003.

Jaffee, Dwight M., and Thomas Russell, "Catastrophe Insurance, Capital Markets, and Uninsurable Risks," *The Journal of Risk and Insurance*, Vol. 64, No. 2, 1997, pp. 205–230.

Kunreuther, Howard, "The Role of Insurance in Managing Extreme Events: Implications for Terrorism Coverage," *Risk Analysis*, Vol. 22, No. 3, 2002, pp. 427-437.

Lanier, Robin, "Testimony of Robin Lanier, Executive Director, the Waterfront Coalition, Before the Water Resources Subcommittee of the Transportation and Infrastructure Committee, U.S. House of Representatives, on the issue of Financing Port Infrastructure," Washington, D.C., November 13 [sic], 2003.

Office of California Senator Christine Kehoe, the California Office of Homeland Security, and the California Association of Port Authorities, Hearing on *Security and California Ports,* Sacramento, California, February 16, 2005.

Organisation for Economic Cooperation and Development, *Terrorism Risk Insurance in OECD Countries*, Policy Issues in Insurance, No. 9, Paris, 2005.
Palm, Risa, "The Roepke Lecture in Economic Geography: Catastrophic Earthquake Insurance: Patterns of Adoption," *Economic Geography*, Vol. 71, No. 2, 1995, pp. 119–131.
"Ports and Harbors: Freight Security Fee," California State Assembly Bill 1406, Introduced by Assembly Member Betty Karnette, Sacramento, California, February 22, 2005.
"Ports: Congestion Relief: Security Enhancement: Environmental Mitigation: User Fee," California State Senate Bill 760, Introduced by Senator Alan Lowenthal, Sacramento, California, February 22, 2005.
"Port Security Improvements Act of 2003," U.S. House of Representatives Bill 2193, Introduced by Representative Doug Ose, Washington, D.C., May 21, 2003.
Rohrabacher, Dana, "Rep. Rohrabacher Testimony on HR 3028: Local Port Discretionary User Fee Authority," Washington, D.C., November 20, 2003.
"Security and Accountability For Every Port Act (SAFE Port Act)," U.S. House of Representatives Bill 4954, Introduced by Representative Dan Lungren and Representative Jane Harman, Washington, D.C., March 14, 2006.
"To Amend the Water Resources Development Act of 1986 to Expand the Authority of Non-Federal Interests to Levy Harbor Fees," U.S. House of Representatives Bill 3028, Introduced by Representative Dana Rohrabacher, Washington, D.C., September 5, 2003.
"To Amend the Water Resources Development Act of 1986 to Expand the Authority of Non-Federal Interests to Levy Harbor Fees," U.S. House of Representatives Bill 494, Introduced by Representative Dana Rohrabacher, Washington, D.C., February 1, 2005.
"United States Seaport Multiyear Enhancement Act," U.S. House of Representatives Bill 3712, Introduced by Representative Juanita Millender-McDonald, Washington, D.C., January 21, 2004.
U.S. Coast Guard, *FY 2003 Report*, Washington, D.C., 2003.
U.S. Coast Guard, *FY 2004 Report*, Washington, D.C., 2004.
U.S. Coast Guard, *FY 2005 Report*, Washington, D.C., 2005.

U.S. Department of Transportation, *2003 Budget in Brief: United States Coast Guard,* Washington, D.C., 2002.
U.S. Department of the Treasury, *Assessment: The Terrorism Risk Insurance Act of 2002,* Report to Congress, Washington, D.C., June 30, 2005.
U.S. Government Accountability Office, *Marine Transportation: Federal Financing and a Framework for Infrastructure Investments, Report to the Chairman, Subcommittee on Surface Transportation and Merchant Marine, Committee on Commerce, Science, and Transportation, U.S. Senate*, GAO-02-1033, Washington, D.C., September 2002.
The White House, Office of Homeland Security, *National Strategy for Homeland Security,* Washington, D.C., July 2002.

Glossary

24-Hour Rule: Requires that ocean carriers provide U.S. Customs and Border Protection with copies of the manifest 24 hours before a container is loaded onto a vessel.

Active Detectors: A non-invasive inspection technology that emits radiation that interacts with items in a container to elicit a detectable response. Also see Passive Detectors.

Adverse Selection: A situation in which people who know that they face a greater risk are more likely to buy insurance than those who face less risk, thereby reducing (or eliminating) the profitability of providing insurance.

Automatic Identification System: A U.S. Coast Guard program established pursuant to the MTSA, which mandates the placement of an electronic identification system on board all vessels in U.S. waters.

Area Maritime Security Committee: A committee established pursuant to the MTSA to bring together stakeholders in the shipping and port communities and assume responsibility for coordinating port security planning for various regions.

Bill of Lading: A document provided by a transportation carrier to a shipper acknowledging that it has received a shipment of goods and that the goods have been put on board a vessel bound for a particular destination.

Bureau of Economic Analysis: A U.S. government agency responsible for providing data and information on the U.S. economy.

Carrier: The company operating one of the many large vessels used to ship products around the world.

Center for Risk and Economic Analysis of Terrorism Events: A center at the University of Southern California, funded by the Department of Homeland Security, to assess the risks and consequences of terrorism.

Community Emergency Response Team: A program of the U.S. Department of Homeland Security dedicated to educating people about disaster preparedness and training them in basic response skills.

Consolidated Metropolitan Statistical Area: A measure of metropolitan area based on county boundaries.

Container: Typically, a 40-foot long (two TEUs) metal box used to ship items around the world.

Consumer Price Index: A measure of price inflation reported by the U.S. Bureau of Labor Statistics.

Container Security Initiative: A U.S. Customs and Border Protection program with four core elements: using intelligence and automated information to identify and screen high-risk containers; inspecting containers identified as high-risk, at the point of departure; using detection technology to quickly inspect high-risk containers; and using smarter, tamper-evident containers. It is best known for screening and inspecting containers at foreign ports.

Customs and Border Protection: The U.S. federal agency in charge of customs and border management and protection for the United States.

Customs Duties: Revenues that result from a tax charged on imported goods.

Customs-Trade Partnership Against Terrorism: A joint government-business initiative that encourages shippers and carriers to implement security plans and measures to promote greater security at all points along the supply chain in exchange for expediting of customs procedures.

Department of Homeland Security: The U.S. federal department in charge of the national network of organizations responsible for U.S. homeland security.

Department of Transportation: The U.S. federal department in charge of the transportation system.

Dirty Bomb: Also known as a radiological dispersal device, consisting of radioactive material combined with explosives with the intent of scattering the material over a wide area.

Environmental Protection Agency: The U.S. agency in charge of protecting human health and the environment.

Externality: Arises when an activity undertaken by one individual affects the welfare of another either positively or negatively. An example of a negative externality is pollution, a byproduct of production that adversely affects the welfare of people other than the producer. An example of a positive externality is a neighbor's well-tended garden, a byproduct of production that benefits people other than the producer.

False Negative: Results when a test indicates that something is *not* present, such as an explosive device or other threat, when in actuality one is present.

False Positive: Results when a test indicates that something *is* present, such as a radiological device or other threat, when in actuality nothing is present.

Federal Emergency Management Agency: Part of the Department of Homeland Security with the mission to prepare for hazards and emergencies as well as taking the lead in response and recovery during emergencies.

Global Positioning System: Uses satellite signals that can be processed via a receiver, which is able to compute position, velocity, and time.

Government Accountability Office: The non-partisan agency in charge of studying the programs and expenditures of the U.S. federal government. Formerly known as the General Accounting Office.

Homeland Security Presidential Directive-13: A presidential directive that mandated the development of a National Strategy for Maritime Security. Several U.S. agencies are involved in the effort, which is led by the National Security Council and the Homeland Security Council. The diretive was also released as National Security Presidential Directive-41.

Incident Command System: A system for managing emergencies developed by the Federal Emergency Management Agency.

International Longshore and Warehouse Union: A union that primarily represents dock workers along the U.S. West Coast, with approximately 42,000 members in over 60 local unions in California, Washington, Oregon, Alaska, and Hawaii.

International Maritime Organization: An agency of the United Nations responsible for international shipping safety and environmental issues.

International Ship and Port Facility Security Code: Established by the International Maritime Organization to provide an international standard for ship and port security.

Input-Output Models: A model based on basic supply and demand theory that uses the fact that the outputs of some industries are the inputs of others, a relationship that can be tracked mathematically.

Intermodal: The use of more than one type of transportation.

Just-in-Time Delivery: An innovation in inventory management whereby inventories are minimized by spreading products out across the supply chain, timed to arrive as nearly as possible to when they are needed.

Manifest: A document or file describing the contents of containers, which accompanies the containers through the supply chain.

Marine Transportation System Task Force: A task force composed of industry associations, shipper groups, and other stakeholders put together in 1999 to assess the marine transportation system.

Maritime Security Levels: A three-tiered system of levels designed to allow the U.S. Coast Guard to respond in a scalable way to increasing terrorist threats.

Maritime Transportation Security Act: Signed on November 25, 2002, and fully implemented on July 1, 2004, a law designed to protect the nation's ports and waterways from a terrorist attack.

Mixed Loads: Containers that contain cargo consisting of many different items originating from several difference sources.

Moral Hazard: The tendency of insurance to change behavior in the direction of greater risk-taking.

National Task Force on Interoperability: An effort by the National Institute of Justice, Office of Science and Technology, to improve public safety communications.

Office of Domestic Preparedness: The principal agency under the federal Department of Homeland Security responsible for preparing the United States for acts of terrorism. ODP is responsible for providing training, funding, and assistance to state and local governments to prevent, plan for, and respond to terrorist acts.

Operation Safe Commerce: A joint U.S. Department of Transportation and U.S. Customs and Border Protection program to fund business initiatives that improve security for container cargo moving within the international transportation system.

Office of Grants and Training: A Department of Homeland Security unit now responsible for the Port Security Grant Program. Formerly known as the Office of State and Local Government Coordination and Preparedness, it also oversees the Office of Domestic Preparedness.

Outer Continental Shelf: The submerged land in the ocean extending beyond the jurisdiction of a state government up to the extent of the federal jurisdiction.

Pacific Maritime Association: Consists of American flag operators, foreign flag operators, and stevedore and terminal companies that operate in California, Oregon, and Washington ports. Its principal business is to negotiate and administer maritime labor agreements with the International Longshore and Warehouse Union.

Panamax Vessel: The maximum-sized vessel that is able to transit the Panama Canal.

Passive Detectors: A non-invasive inspection technology that does not interact with cargo but instead "passively" senses trace radiation that may exist.

Primary Metropolitan Statistical Area: A subdivision of a CMSA.

Port Security Grant Program: Provides federal financing for physical security enhancements at large U.S. ports.

Post-Panamax Vessel: A vessel whose large size does not allow it to transit the Panama Canal, unlike a Panamax vessel.

Public Good: A good that is difficult to produce for private gain because no one can be excluded from its use and because one person's use does not diminish another person's use. An example is national defense.

Radiation Portal Monitor: A broad category of radiation detection equipment, some types of which are being implemented at U.S. seaports.

Radiological Dispersal Device: Also known as a dirty bomb, consisting of radioactive material combined with explosives with the intent of scattering the material over a wide area.

Radio Frequency Identification: A way of storing and retrieving data using small tags that can be placed onto or into a product. RFID tags have antennas to receive and respond to radio frequency signals from an RFID transceiver.

Roentgen Equivalent Man: A measure of radiation exposure.

Safety of Life at Sea: An International Maritime Organization convention, originally convened in 1929, that dictates standards for safety on cargo and passenger ships.

Sarin: A toxic substance similar to some insecticides that is classified by the United Nations as a weapon of mass destruction.

Southern California Association of Governments: The metropolitan planning organization for six counties: Los Angeles, Orange, San Bernardino, Riverside, Ventura, and Imperial.

Shipper: The company in charge of a container or product being shipped, usually the entity that is taking delivery, such as Wal-Mart or Target.

Smart Card: Resembles a credit card in size and shape and uses a microprocessor to store and track information for a variety of purposes.

Teamsters: One of the largest labor unions in the United States, known for representing truck drivers but also for representing many port workers and other groups.

Terrorism Information Awareness Program: A U.S. Defense Department research project that aims to identify terrorists by analyzing personal data collected in computer databases; previously known as the Total Information Awareness Program.

Terminal: The area of a port complex nearest the water, where cargo is loaded and unloaded from vessels.

Terminal Island: An island shared by the Port of Long Beach and the Port of Los Angeles that is the home of many container and bulk terminals.

Total Information Awareness Program: A U.S. Defense Department research project that aims to identify terrorists by analyzing personal data collected in computer databases; now known as the Terrorism Information Awareness Program.

Transportation Security Administration: A U.S. Department of Homeland Security agency responsible for protecting the nation's transportation systems.

Transportation Security Administration Maritime Self-Assessment Risk Module: Developed in response to mandates in the MTSA, guides a port or vessel security officer through questions to develop a measure of the vulnerability of a port facility or vessel to terrorist threats.

Transportation Worker Identification Credential: An identification card being developed for transportation workers of all types who must have access to secure areas.

Twenty-Foot Equivalent Unit: A measure of containerized cargo equal to one standard 20 foot (length) by 8 foot (width) by 8.5 foot (height) container.

United States Coast Guard: One of the five U.S. military branches; responsible for maritime and coastal security as well as various humanitarian and law enforcement duties. It is a part of the Department of Homeland Security.

Universal Product Code: A product marking technology using a bar code sequence.

Urban Areas Security Initiative: A program in the U.S. Department of Homeland Security that provides financing to help urban areas build capacity to prevent, respond to, and recover from terrorist activities.

User Fees: Fees charged for use of a service.

Very-Large-Scale Integrated Device: A semiconductor chip that includes many tens of thousands of transistors. This term has become somewhat quaint now that virtually all chips exceed this number of transistors.

Wi-Fi: Short for wireless fidelity; used as shorthand for any of a variety of wireless communication networks.

Weapons of Mass Destruction: Nuclear, biological, radiological, or chemical weapons.

About the Authors

STEPHEN S. COHEN

Stephen S. Cohen is a professor at the University of California, Berkeley, where he is co-director and co-founder of the Berkeley Roundtable on the International Economy (BRIE). He has published several books, articles in academic journals such as *American Economic Review*, *California Management Review*, and *SCIENCE*, as well as articles in more popular journals such as *Foreign Affairs*, *Les Temps Modernes*, *The Wall Street Journal*, *The Harvard Business Review,* and *The Atlantic Monthly*. He has served as adviser to the White House on diverse matters and to several committees of Congress, as well as to the presidents of the European Union, Spain, and Brazil; several foreign governments; the United Nations; the Organisation for Economic Co-Operation and Development; and many companies in the United States, Japan, and Europe. He completed his B.A. at Williams College and his Ph.D. at the London School of Economics. A member of the UC Berkeley faculty since 1968, he has been honored with the Medal of Paris and with visiting fellowships and professorships at the Massachusetts Institute of Technology, Harvard University, New York University, the University of Toronto, l'Ecole Nationale d'Administration, and the Sorbonne.

PETER GORDON

Peter Gordon is a professor in the University of Southern California's (USC's) School of Policy, Planning and Development and in its Department of Economics. He is also director of USC's Master of Real Estate Development program and is affiliated with the university's Center for Risk and Economic Analysis of Terrorism Events. His work includes the development of economic impact models and their application. He has also published widely on the relationships between urban structure and personal transportation choices. He received his Ph.D. from the University of Pennsylvania.

JON D. HAVEMAN

Jon D. Haveman is a research fellow and director of the Economy Program at the Public Policy Institute of California. He is a specialist in the effects of international barriers to trade, international competition policy, and transportation and security issues as they pertain to servicing internationally traded goods. He is the author of the PPIC report *California's Global Gateways: Trends and Issues* and of more than 25 published articles in the area of international trade. These include *The Benefits of Market Opening, The Determinants of Long Term Growth*, and *The Effects of U.S. Trade Laws on Poverty in America*. He was previously on the faculty of the Economics Department at Purdue University, has served as the Senior International Economist on the President's Council of Economic Advisers, and has been a visiting fellow at the U.S. Bureau of the Census. He has also worked as a research economist at the Federal Trade Commission's Bureau of Economics. He holds a B.A. in economics from the University of Wisconsin, Madison, and an M.S. and Ph.D. in economics from the University of Michigan.

MATTHEW C. HIPP

Matthew C. Hipp is a J.D. candidate at the University of California Los Angeles School of Law. He served for seven years as an officer in the U.S. Navy. He holds an M.P.P. from the UCLA School of Public Affairs, where his team's applied policy project, entitled *Port Security: Recommendations to Improve Emergency Response Capabilities at the Port of Los Angeles and the Port of Long Beach*, received highest honors.

SETH K. JACOBSON

Seth K. Jacobson consults on counterterrorism issues in Los Angeles County including the ports of Los Angeles and Long Beach, where he serves on the Area Maritime Security Subcommittee for Training and Exercises. He earned an M.P.P. from the UCLA School of Public Affairs, where his team's applied policy project, entitled *Port Security: Recommendations to Improve Emergency Response Capabilities at the Port of Los Angeles and the Port of Long Beach*, received highest honors. He holds an MBA from UCLA and an A.B. in astronomy and astrophysics from Harvard.

EDWARD E. LEAMER

Edward E. Leamer is the Chauncey J. Medberry Professor of Management, professor of economics, and professor of statistics at UCLA, and director of the UCLA Anderson Forecast. After serving as assistant and associate professor at Harvard, he joined UCLA in 1975 and served as chair of the Economics Department from 1983 to 1987. In 1990, he moved to the Anderson Graduate School of Management. He received a B.A. in mathematics from Princeton University and an M.A. in mathematics and a Ph.D. in economics from the University of Michigan. He has published four books and more than 100 articles. His research papers in econometrics have been collected in *Sturdy Econometrics*, published in the Edward Elgar Series of Economists of the 20th Century. His research in international economics and econometric methodology has been discussed in *New Horizons in Economic Thought: Appraisals of Leading Economists*. He is a fellow of the American Academy of Arts and Sciences and a fellow of the Econometric Society. He is also a research associate of the National Bureau of Economic Research and currently is on the advisory board of the Bureau of Economic Analysis of the U.S. Commerce Department.

JAMES E. MOORE, II

James E. Moore, II, is professor of Industrial and Systems Engineering, Civil Engineering and Public Policy and Management, and chair of the Epstein Department of Industrial and Systems Engineering at USC. He specializes in transportation engineering, transportation systems, and other infrastructure systems. He is director of the Transportation Engineering program and co-director of the Construction Management program. His research interests include risk management of infrastructure networks subject to natural hazards and terrorist threats; economic impact modeling; transportation network performance and control; large-scale computational models of metropolitan land use/transport systems, especially those in California; evaluation of new technologies; and infrastructure investment and pricing policies. In 2003, he was elected to the Russian Academy of Natural Sciences, United States Section, for outstanding contributions to the field of transportation systems engineering and received the Kapitsa Gold Medal of Honor.

QISHENG PAN

Qisheng Pan is an associate professor in the Department of Urban Planning and Environmental Policy at Texas Southern University. His major research interests include quantitative analysis, transportation planning, spatial analysis, and Geographic Information Systems applications in urban and environmental planning. He received a B.S. in geology and an M.S. in cartography and remote sensing from Peking University, Beijing, and an M.S. in computer science and a Ph.D. in urban and regional planning from USC. He has worked on multiple research projects funded by the National Center for Metropolitan Transportation Research and the Center for Risk and Economic Analysis of Terrorism Events at USC, the California Department of Transportation, the Texas Department of Transportation, and the National Science Foundation. His most recent research includes the measure of access to public transportation services, the economic impacts of terrorist attacks, and a dynamic composition of web services for goods movement analysis.

HARRY W. RICHARDSON

Harry W. Richardson is the James Irvine Chair of Urban and Regional Planning in the School of Policy, Planning and Development and a professor of economics at USC. He is focusing much of his current research efforts on the economics of terrorism under the SPPD-Viterbi School of Engineering's CREATE banner. He is co-editor of the book *The Economic Impacts of Terrorist Attacks*, published in 2005 by Edward Elgar, and of two forthcoming books on terrorism, *The Economic Costs and Consequences of Terrorist Attacks*, which is in the copy-editing stage, and *The Risk and Economics of Katrina*, which is in the planning stage. He was an Overseas Visiting Fellow at Churchill College, Cambridge University, in fall 2004 and in spring 2006, researching urban regeneration and London's congestion pricing scheme. In addition, he was recently given the Walter Isard Award for Scholarly Achievement in Regional Science by the Regional Science Association International. He is also doing research on the origins of regional economics and on Korean reunification.

HOWARD J. SHATZ

Howard J. Shatz is a research fellow at the Public Policy Institute of California, where he focuses on California's interactions with the global economy. His research interests include foreign direct investment,

international trade, international economic development, and seaport security. He has worked as a consultant to the World Bank and has held research fellowships at the Brookings Institution and the Board of Governors of the Federal Reserve System. He is the author of the PPIC reports *Business Without Borders? The Globalization of the California Economy* and *The Emerging Integration of the California-Mexico Economies* (with Luis Felipe López-Calva). He has also written journal articles and book chapters about trade and labor markets, exchange rates and economic performance, the geography of international investment, trade barriers and low-income countries, and services trade. He has testified before state and federal legislative committees about California's foreign trade offices, government assistance for international business development, and California-Mexico economic relations and has worked on advisory projects for countries in Latin America, Africa, and South Asia. He holds a Ph.D. in public policy from Harvard.

JAY STOWSKY

Jay Stowsky is a senior research associate at the Berkeley Roundtable on the International Economy (BRIE) at UC Berkeley, where he also serves as special assistant to the vice provost for academic planning and facilities. He served in the Clinton administration as senior economist for science and technology policy on the staff of the White House Council of Economic Advisers. He has authored several studies of U.S. technology policy and the commercial effects of military-funded research and development. He served previously as associate dean at UC Berkeley's Haas School of Business and as director of research policy for the University of California system. He holds an M.P.P. from Harvard's Kennedy School of Government and a Ph.D. in regional planning from UC Berkeley.

CHRISTOPHER THORNBERG

Christopher Thornberg is a senior economist with the UCLA Anderson Forecast and authors the Anderson Forecast for California as well as for the Los Angeles and East Bay regions. He specializes in international and labor economics. He has been involved in a number of special studies measuring the effect of important events on the economy, including the North American Free Trade Agreement, the California power crisis, and the September 11 terrorist attacks. He received his B.S. in business administration from the State University

of New York at Buffalo and his Ph.D. in business economics from the Anderson School. He was previously on the faculty of the Economics Department at Clemson University.

ERNESTO VILCHIS

Ernesto Vilchis is a dual master's degree candidate in public affairs and urban and regional planning at the Woodrow Wilson School of Public and International Affairs at Princeton University. He previously served as a research associate at PPIC, where he conducted research on international trade, Mexico-U.S. border issues and economic relations, and port security. He has written journal articles, book chapters, and other publications on international trade, port security, rural poverty in Mexico, and land tenure issues in Latin America. He earned his B.A. in economics from UC Berkeley.

AMY B. ZEGART

Amy B. Zegart is associate professor of public policy at UCLA. She has written widely about organizational problems in U.S. national security agencies. Her first book, *Flawed by Design: The Evolution of the CIA, JCS and NSC*, published by Stanford University Press, won the Leonard D. White Award, given to the best dissertation in the field of public administration, from the American Political Science Association. Her forthcoming book, *Intelligence in Wonderland,* to be published in 2007, examines why the CIA and FBI adapted poorly to the rise of terrorism after the Cold War. She spent three years at McKinsey & Company, where she advised *Fortune* 100 companies about strategy and organizational effectiveness. She holds a Ph.D. in political science from Stanford University and currently serves on the Los Angeles/Orange County Homeland Security Advisory Committee.

Related PPIC Publications

Federal Formula Grants and California: Homeland Security
Tim Ransdell

California's Global Gateways: Trends and Issues
Jon D. Haveman, David Hummels

Local Homeland Security in California: Surveys of City Officials and State Residents
Mark Baldassare, Christopher Hoene, Jonathan Cohen

Local Homeland Security and Fiscal Uncertainty: Surveys of City Officials in California
Mark Baldassare, Christopher Hoene

PPIC publications may be ordered by phone or from our website
(800) 232-5343 [mainland U.S.]
(415) 291-4400 [outside mainland U.S.]
www.ppic.org