CENTER FOR TERRORISM
RISK MANAGEMENT POLICY

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Browse Books & Publications
Make a charitable contribution

For More Information

Visit RAND at www.rand.org
Explore RAND Center for Terrorism Risk Management Policy
View document details

Limited Electronic Distribution Rights
This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use.
This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.
Economically Targeted Terrorism

A Review of the Literature and a Framework for Considering Defensive Approaches

Brian A. Jackson, Lloyd Dixon, Victoria A. Greenfield
The research described in this report was conducted within the RAND Center for Terrorism Risk Management Policy (CTRMP).

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2007 RAND Corporation

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from RAND.

Published 2007 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org
Since September 11, 2001, a great deal of attention has been focused on the economic consequences of terrorism. It has come not only from individuals and organizations responsible for combating terrorism who want to understand how to reduce the economic damage that terrorist action can cause to a nation, but from terrorists as well. Following the significant costs of the September 11 attacks, economic targeting—the desire to intentionally create economic damages significant enough to hurt or influence a targeted nation—took a more prominent place in the statements of Osama bin Laden and like-minded terrorists targeting the United States.

This document examines the economic consequences of terrorism. It focuses on understanding the elements that might shape terrorist decisionmaking if inflicting economic damages is a primary goal, as well as on laying out the range of defensive approaches that might be taken to protect nations from economic targeting.

The report should be of interest to federal and state policymakers, insurers, commercial organizations, and others who have a stake in ensuring the economic security of the United States in the face of the terrorist threat.

The research reported here was supported by the RAND Center for Terrorism Risk Management Policy (CTRMP) as part of its larger research program focused on terrorism risk, insurance, and other related economic issues.

The RAND Center for Terrorism Risk Management Policy (CTRMP)

CTRMP provides research that is needed to inform public and private decisionmakers on economic security in the face of the threat of terrorism. Terrorism risk insurance studies provide the backbone of data and analysis to inform appropriate choices with respect to government involvement in the market for terrorism insurance. Research on the economics of various liability decisions informs the policy decisions of the U.S. Congress and the opinions of state and federal judges. Studies of compensation help Congress to ensure that appropriate compensation is made to the victims of terrorist attacks. Research on security helps to protect critical infrastructure and to improve collective security in rational and cost-effective ways.
CTRMP is housed at the RAND Corporation, an international nonprofit research organization with a reputation for rigorous and objective analysis and the world’s leading provider of research on terrorism. The center combines three organizations:

- RAND Institute for Civil Justice, which brings a 25-year history of empirical research on liability and compensation
- RAND Infrastructure, Safety, and Environment, which conducts research on homeland security and public safety
- Risk Management Solutions, the world’s leading provider of models and services for catastrophe risk management.

For additional information about the Center for Terrorism Risk Management Policy, contact

Robert Reville  
RAND Corporation  
1776 Main Street  
P.O. Box 2138  
Santa Monica, CA 90407  
Robert_Reville@rand.org  
310-393-0411, x6786

Michael Wermuth  
RAND Corporation  
1200 South Hayes Street  
Arlington, VA 22202  
Michael_Wermuth@rand.org  
703-413-1100, x5414

A profile of the CTRMP, abstracts of its publications, and ordering information can be found at http://www.rand.org/multi/ctrmp/.
Jeffrey DeBoer (Co-Chair)  
President and Chief Executive Officer  
Real Estate Roundtable

Pierre L. Ozendo (Co-Chair)  
Member of the Executive Board, 
Head of Americas Property and Casualty 
Swiss Re America Holding Corporation

Jack Armstrong  
Assistant Vice President and 
Senior Regulatory Counsel 
Liberty Mutual Insurance Company

Brian Boyden  
Executive Vice President 
State Farm Insurance

Andrew Coburn  
Vice President of Catastrophe Research and 
Director of Terrorism Research 
Risk Management Solutions, Inc.

Kenneth Feinberg  
Managing Partner 
The Feinberg Group, LLP

Ken Jenkins  
Chief Underwriting Officer 
American Reinsurance RiskPartners

Peter Lowy  
Chief Executive Officer 
Westfield Corporation, Inc.

Kathleen Nelson  
Immediate Past Chair 
International Council of Shopping Centers (ICSC)

Art Raschbaum  
Executive Vice President and Managing Director 
GMAC RE

Kevin Scroggin  
General Director,  
Corporate Risk Management and Insurance 
General Motors

Hemant Shah  
President and Chief Executive Officer 
Risk Management Solutions, Inc.

Cosette Simon  
Senior Vice President 
Swiss Re Life and Health America, Inc.

Richard Thomas  
Senior Vice President and 
Chief Underwriting Officer 
American International Group

Steven Wechsler  
President and Chief Executive Officer 
National Association of Real Estate Investment Trusts (NAREIT)
## Contents

Preface ................................................................. iii  
Center for Terrorism Risk Management Policy Advisory Board ....................................... v  
Figures ................................................................. ix  
Tables ................................................................... xi  
Summary .............................................................. xiii  
Acknowledgments ................................................ xix  
Abbreviations ....................................................... xxi

### CHAPTER ONE

**Introduction** .................................................. 1  
Defining Economic Targeting as an Element of Terrorist Operations ............................... 2  
Two Types of Economic Targeting: Episodic Terrorism Versus Terrorist Campaigns ....... 3  
About This Report .................................................. 4

### CHAPTER TWO

**The 9/11 Attacks: The Economic Costs of High-Impact Terrorism** .............................. 7  
The Economic Effects of the September 11, 2001, Attacks ........................................ 7  
Discussion .............................................................. 10

### CHAPTER THREE

**PIRA in Northern Ireland: Adding Up the Costs of a Long-Term Conflict** ............... 13  
The Economic Effects of the PIRA Terrorist Campaign ............................................ 14  
PIRA Operations in Northern Ireland ................................................................. 14  
PIRA Operations on the UK Mainland .............................................................. 17  
Discussion .............................................................. 19

### CHAPTER FOUR

**A Framework for Understanding the Economic Costs of Terrorism** ....................... 22  
Economically Targeted Terrorism Generates Three Types of Costs ............................. 22  
Attack Costs .......................................................... 23  
Security and Preparedness Costs ............................................................................. 23  
Behavioral Change Costs ....................................................................................... 24
Understanding What Determines the Economic Costs of Terrorism: What Factors Drive Increases in Costs? ......................................................................................... 25
The First Main Driver of Economic Costs: A Terrorist Group’s Ambition to Stage a Large-Scale, High-Cost Attack .............................................................. 25
The Second Main Driver of Economic Costs: Perceptions That the Risk of Terrorism Is High ............................................................. 27
Linking the Perception of Risk to Economic Costs: Two Ways in Which Fear Can Become Costly ........................................................................................................ 29
Changes in Behavior in Response to the Risk of Terrorism ................................................................. 30
Increases in Demand for Security and Preparedness Measures .......................................................... 34
Summary ..................................................................................................... 35

CHAPTER FIVE
Defending Against Economically Targeted Terrorism .................................................... 37
Two Policy Levers to Guide National Responses to Economic Targeting ............................ 37
Security and Preparedness Measures ........................................................................ 38
Robustness and Resilience Measures ...................................................................... 39
Insurance and Compensation .............................................................................. 42
Public Information and Risk Communication .......................................................... 43
Issues to Consider in Crafting a Defensive Plan ........................................................... 45
How Do Measures Perform in a Varying and Uncertain Threat Environment? ............... 45
How Do Measures Perform Over Time? ................................................................... 46
How Do Measures Reconcile National and Local, or Public and Private Incentives for Preparedness? ........................................................................ 47
How Do Measures Shape Behavior Within the Economy? .............................................. 47

CHAPTER SIX
Conclusions ............................................................................................... 49
Bibliography .............................................................................................. 51
Figures

S.1. Conceptual Framework for Examining Economically Targeted Terrorism ............... xvii
   4.1. Drivers of Attack Costs ......................................................... 26
   4.2. Drivers of Security and Preparedness and Behavioral Change Costs............... 28
   4.3. Conceptual Framework for Examining Economically Targeted Terrorism ............ 36
Tables

4.1. Potential Economic Costs of Terrorism for Government, Businesses, and Individuals ... 25
5.1. Insurance and Compensation Mechanisms for Reallocating Costs from Terrorism ..... 43
Though attention on the threat of terrorism frequently focuses on the deaths and injuries caused in terrorist attacks, acts of violence can also cause economic harm. Since September 11, 2001, al Qaeda leaders have singled out the U.S. economy as a target for attack. Though prominent in contemporary terrorism, economic targeting is not a new phenomenon. Terrorist groups with very different goals from al Qaeda’s—such as the Provisional Irish Republican Army (PIRA) in Northern Ireland and England—have used economic coercion and damage as elements of their campaigns for many years. By exploring these past cases and building a framework identifying the costs of terrorism and their drivers, this report provides a basis for crafting effective defensive strategies for nations whose economies terrorist groups target.

A Spectrum of Economic Targeting By Terrorist Organizations

We define economic targeting as a terrorist group’s intent to inflict economic costs on a targeted state by doing one or both of two things:

- threatening to destroy or damage property\(^1\) or harm people
- actually destroying or damaging property or harming people.

For a specific terrorist action, causing economic damage may be a group’s primary intent or may be only one of a range of goals the group has in mind.

Terrorists have taken a variety of approaches to economic targeting. The 9/11 attacks by al Qaeda and PIRA’s economic targeting activity define two ends of a spectrum:

- isolated high-profile, high-impact attacks (9/11)
- campaigns of repeated smaller-scale incidents (PIRA).\(^2\)

---

\(^1\) We define property as “systems and assets, whether physical or virtual” (see Public Law 107-56, p. 401). Assets also include productive capital and goods in inventory or pipeline.

\(^2\) In fact, these are two of four extreme cases: (1) high-frequency, low-intensity terrorism (campaign terrorism), (2) low-frequency, high-intensity terrorism (episodic terrorism), (3) low-frequency, low-intensity terrorism, and (4) high-frequency, high-intensity terrorism. Cases 3 and 4 are less relevant for policy consideration, however. In case 3, the economic impact would be small and therefore of much less concern. Case 4 is of limited probability given the capability constraints of non-
An individual high-profile terrorist attack such as 9/11—to which we refer as episodic terrorism—occurs at a defined point in time. Attack planners design it to generate large economic costs. After the attack is carried out, its effects travel through an economy, producing additional costs, in some cases decaying and in others persisting over time. In contrast, in an extended terrorist conflict such as PIRA’s—which we call campaign terrorism—the occurrence of each individual terrorist event and the costs it produces are less important than the expectation that the group will repeat the violence. Recurrent violence becomes a feature of the economic environment. In campaign terrorism, attack planners design costs to build up and compound over time, rather than stem from one specific attack.

Three Classes of Economic Costs

The different types and magnitudes of costs produced in those two examples of economic targeting provide the basis for building a framework laying out how the costs of terrorism build up and how different costs relate to one another. The costs of economic targeting can be divided into three classes:

- the costs of the attack itself, including damage to structures or other capital, costs of individuals killed and injured, and cascading effects within and among sectors from damages that affect other firms’ operations
- the costs of implementing security and preparedness measures in response to the potential for future attacks, including all expenditures for security, response and recovery measures, and indirect costs associated with those measures (e.g., increased wait times for security searches, inefficiencies in transport or supply chains)
- the costs resulting from changes in behavior due to the perception of the threat of future attacks, including reductions in demand due to fear or uncertainty, changes in demand due to the behavior of financial markets or the value of assets, shifts in investment behaviors due to changed risk perceptions, and other second-order economic costs produced by changes in activity resulting from terrorism.

Within each category, these costs can accrue to government, businesses, and individuals.

What Drives the Costs of Terrorism?

To provide a basis for defensive planning, we must understand what factors determine the scale of the costs of economic targeting. A simple model can be constructed in which two components drive the costs of terrorism:

---

state terrorist groups. It instead more closely resembles interstate war. If it did occur, it would demand of governments such drastic changes and measures that discussing its costs to the ex ante economy is not terribly meaningful.
• a terrorist group’s desire to maximize attack costs and its ability to use particular attack
modes or exploit key vulnerabilities to do so
• government, business, or individual perceptions that the risk of terrorism is high, pro-
ducing both demand for security and preparedness expenditures and costs arising from
behavioral changes.

Attack costs are purely incident-driven: The adversary’s desire to inflict economic harm,
its choice of tactics and target, and the target’s vulnerability shapes these costs. Beyond simply
attempting to “scale up” their attacks, a second strategy for a group to maximize these costs is
to stage operations with cascading effects that magnify the immediate damage and extend it
over time.

The goal of generating fear lies at the heart of terrorism. Economic targeting is no excep-
tion to this rule. To understand economic targeting, it is useful to think about the perception
of risk as being a function of two factors:

• *Perceptions of the terrorist threat:* Organizations and individuals build expectations about
  the nature of future attacks. They develop beliefs about the likely type, frequency, and
  location of attacks—whether attacks are likely, what scale and type of damages will result,
  how frequently they will occur, where they are likely to take place, and what are likely
  targets. The perceived threat may or may not reflect the actual level of terrorist threat.
• *Perceptions of the effectiveness of security and preparedness measures:* Effective measures can
  cause attacks to fail, limit an attack’s effects, and reduce the chance that the same terrorist
  group will wage repeat attacks. Individuals and organizations develop beliefs about how
  effective current security and preparedness measures are.

In this simplified construct, risk is perceived if the level of effectiveness of security mea-
sures is considered insufficient to negate the perceived terrorist threat. The *match* between
the perceptions of threat and of security is what is important: Whatever the perceived level of
threat, if people believe that the security measures in place are enough to address it and the
two are appropriately balanced, then they judge the situation as generally secure, and they will
perceive risk as minimized or eliminated. If they see the two as not well balanced, a perception
of insecurity will result.

A perception of risk can produce behavioral changes, leading to economic costs. Simi-
larly, fear can increase the demand for security and preparedness expenditures, compelling
government and businesses to take measures to protect against the threat. These security and
preparedness measures can be costly, contributing to the overall economic cost of terrorism.

The most direct and obvious way in which a terrorist group can manipulate this balance
in its favor is successfully staging an attack: An event that the public may have previously
deemed unlikely becomes perceived as a much higher probability. In reality, this may or may
not be the case, although, in the aftermath of an attack, a terrorist group may take actions to
reinforce the idea that future attacks should be viewed as more likely. As for security measures,
people tend to view their effectiveness in a binary fashion: Either they succeed in preventing
attacks or they do not. This is not necessarily the only or most appropriate way to view the
performance of security measures. But when a successful terrorist attack occurs, people who adopt this view will likely decide that, by definition, whatever security measures were in place at the time have failed. This affects the other side of this balance, also leading to a perceived increase in terrorism risk.

A Framework Linking the Economic Costs of Terrorism and Their Drivers

Figure S.1 brings together the three categories of costs associated with economic targeting and illustrates their interrelationships. Attack costs are driven by the combination of a terrorist group’s intent to cause large-scale damage and whether or not current security and preparedness measures leave vulnerabilities in a potential target that the group can exploit to produce significant economic costs. Without a successful attack, there will be no attack costs. In contrast, costs in the other two categories can accrue whether or not an attack actually occurs. If government, businesses, or individuals perceive a risk of attack (resulting from a perceived mismatch between the level of threat and current security and preparedness efforts), the outcome may be an increase in demand for security and preparedness expenditures, costs produced by behavioral changes, or both. In shaping the overall cost of economically targeted terrorism, security and preparedness investments are key, for, as additional investments are made, they feed back to affect both potential attack costs (assuming that they are effective) and the perception of the risk of terrorism (assuming that they are perceived to be effective.)

Defending Against Economically Targeted Terrorism

Clear policies addressing the economic damage from terrorism and, ideally, limiting terrorist groups’ ability to successfully harm an economy, are an important part of a comprehensive defensive effort against terrorism. Preparing the nation for economically targeted terrorism presents considerable challenges, however. Implementing a defensive strategy to protect the nation requires action not just by government, but by individuals and firms as well. Just as each can be a victim of economic targeting, each has a role in defending against it. In some cases, actions that an independent party may take to protect itself will also serve to protect the nation more broadly. But often, individual and national interests do not coincide. For a response to economic targeting to be successful at the national level, government, businesses, and individuals at all levels within an economy must have clear incentives and guidance for responding to this threat in ways that work together to serve the national interest.

The two main drivers of the costs of terrorism point, in turn, to two possible policy levers that might be used to shape public, private, and citizen responses to this threat:

• The first and most straightforward is to reduce the potential attack costs of future events. One approach is to lower the probability of a successful attack; another is to limit the consequences of attacks that are successfully carried out.
Figure S.1
Conceptual Framework for Examining Economically Targeted Terrorism

First cost driver

Terrorist intent to cause economic harm

Perceived threat level

Balanced?

Second cost driver

Imbalance causes perceived terrorism risk

Perceived security and preparedness effectiveness

Demands for more security and preparedness

Changes in economic behavior

Behavioral change costs

Feedback to level of

Vulnerable target

Current security and preparedness measures

Security and preparedness costs

Change in economic behavior

- The second is to take actions that shift the perceived level of terrorist risk, thereby reducing the potential for security and preparedness and behavioral change costs.

We present four options that illustrate the range of tactics that might be used to apply these two levers:

- **Security and preparedness measures**: Because measures in this category can directly reduce the immediate costs of attacks, decisionmakers frequently give them priority. But because these measures come with a price tag, caution is needed so that the resources devoted to them do not end up generating the very costs that a terrorist group aims to impose.

- **Robustness and resilience measures**: The robustness of an economy (as well as particular networks within it) is its ability to limit the damage of an attack by failing in ways that will contain the attack’s effects to the fullest extent possible. Robustness can be built through a variety of mechanisms. The design of infrastructure networks can be changed to reduce their vulnerability to large-scale failures, for example. Resilience has been defined as an

---

3 Although the full range of approaches to the problem of terrorism—including, for example, intelligence and law enforcement action—helps reduce the potential economic damages from attack, addressing all such strategies is beyond the scope of this document. These broader counterterrorism activities clearly contribute to the effectiveness of the more purely economic approaches we describe here and should be examined and assessed in tandem with them.
economy’s ability to reduce the damages that occur from a severe shock by rapidly adjusting to and addressing its consequences.

- **Insurance and compensation:** Compensation and insurance provide ways for the costs suffered by government, firms, and individuals directly affected in an attack to be transferred to others within the economic system. The rationale for reallocating costs in this way is twofold: to provide the resources needed for affected businesses and individuals to recover more rapidly (or, depending on their scale, make it possible to recover at all) and to reduce any additional costs that might result from changes in behavior made in response to the initial costs.

- **Public information and risk communication:** Efforts to communicate with the public about the terrorist threat and security and preparedness measures and to provide other relevant information have the potential to shape individuals’ and firms’ perceptions of the level of terrorism risk and guide their behaviors in response to those perceptions. But efforts to disseminate public information must be implemented carefully. If the information provided does not, in fact, reflect actual levels of threat or preparedness, it has the potential to create unnecessary costs by generating a demand for more security or producing additional behavioral change costs.

All four types of actions are examples of ways in which these policy levers can be used to either reduce the attractiveness of economic targeting as a strategy or limit its effectiveness if adversaries seek to carry out economically focused attacks. However, when a terrorist group’s goal is to cost a targeted nation money and money must be spent to address the threat, crafting a strategy in which money is spent wisely is not just good stewardship, but an integral part of successfully carrying out the counterterrorism mission. Failure to do so risks contributing to the terrorists’ goals rather than our own.
The authors would like to acknowledge a number of RAND colleagues who contributed to this work. John MacDonald, David R. Frelinger, and Henry H. Willis generously contributed their expertise to help refine and strengthen elements of the discussion. We also acknowledge the involvement of a number of RAND research staff and management in shaping the report and would like to particularly and gratefully acknowledge the contributions of Paul Steinberg and Susan Bohandy of RAND’s research communications group for their efforts. We would also acknowledge the inputs of Darius Lakdawalla of RAND and Michael Intriligator of the University of California, Los Angeles, who were involved in reviewing the report. All shortcomings obviously remain the sole responsibility of the authors.
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBO</td>
<td>U.S. Congressional Budget Office</td>
</tr>
<tr>
<td>CTRMP</td>
<td>Center for Terrorism Risk Management Policy</td>
</tr>
<tr>
<td>ETA</td>
<td>Euskadi Ta Askatasuna, or Basque Fatherland and Liberty</td>
</tr>
<tr>
<td>FARC</td>
<td>Fuerzas Armadas Revolucionarias de Colombia, or Revolutionary Armed Forces of Colombia</td>
</tr>
<tr>
<td>FDI</td>
<td>foreign direct investment</td>
</tr>
<tr>
<td>LTTE</td>
<td>Liberation Tigers of Tamil Eelam</td>
</tr>
<tr>
<td>NAICS</td>
<td>North American Industry Classification System</td>
</tr>
<tr>
<td>PIRA</td>
<td>Provisional Irish Republican Army</td>
</tr>
<tr>
<td>TRIA</td>
<td>Terrorism Risk Insurance Act</td>
</tr>
</tbody>
</table>
When a terrorist group\(^1\) succeeds in carrying out a violent attack, attention is instantly riveted on the human casualties and structural devastation. People first measure the attack’s impact in these shocking and immediate terms. But the assault can also produce less visible damage: Acts of violence can be used to bring about economic harm—to great effect.

Terrorism directed toward this end is a topic of increasing concern.\(^2\) Since September 11, 2001, al Qaeda leaders—Osama bin Laden in particular—have specifically identified the U.S. economy as a target:

> It is important to hit the economy (of the United States), which is the base of its military power. . . . (BBC News, 2001c)

> This economic hemorrhaging . . . requires more blows. . . . [T]he youth should try to find the joints of the American economy and hit the enemy in these joints, with God’s permission. (CBS News, 2001)

The success of al Qaeda’s attacks in 2001 on the Pentagon and the World Trade Center brought this issue front and center. Bin Laden assessed 9/11’s economic consequences in no uncertain terms:

> The [9/11] operations have brought about the largest economic crisis that America has ever known. Material losses amount to one trillion dollars. America has lost about two thousand economic brains as a result of the operations. The stock exchange dropped drastically, and American consumer spending deteriorated. The dollar has dropped, the airlines have been crippled, the American globalization system, which was going to spoil the world, is gone. . . . (bin Laden, quoted in Cullison, 2004)

---

\(^1\) In this report, we adopt the convention that terrorism is a tactic—the systematic and premeditated use, or threatened use, of violence by nonstate groups to further political or social objectives to coerce an audience larger than those directly affected. It follows that individual organizations are not inherently “terrorist.” We use the terms terrorist group and terrorist organization as shorthand for “group that has chosen to utilize terrorism.”

\(^2\) See the discussions in Saxton (2002a) and Hunt (2007).
Since 2001, like-minded terrorists have exhorted their fighters to inflict economic damage on the United States and its allies.³

Designing attacks to impair the economy of a targeted state is not a new phenomenon, however, nor is it associated only with terrorist groups active today. The Provisional Irish Republican Army (PIRA), for example, was an organization with aims and practices very different from those of al Qaeda and its affiliates. Throughout its more than 30-year campaign, it used economic targeting as part of its strategy (Rogers, 2000), staging a variety of operations designed to hurt both the economy of Northern Ireland and the UK economy more broadly. The group directly attacked energy infrastructures and UK ships transporting coal. One of its most devastating attacks was a large-scale bombing of London's financial district. While al Qaeda and PIRA differ markedly in many ways, the parallel between the PIRA operations and al Qaeda's attacks on energy production facilities in Saudi Arabia and the World Trade Center in New York's financial hub is striking.⁴

Defining Economic Targeting as an Element of Terrorist Operations

Traditional views on the nature of terrorism held that terrorists’ power to achieve their goals came primarily from how an “audience”—usually political decisionmakers and the public—react to the attacks they carry out, rather than in any direct damage that the attacks themselves produce. This perspective stems from the fact that terrorist organizations are almost always greatly overmatched by the states they target; the asymmetry between the resources of nonstate groups and state militaries means that it is usually impossible for terrorist groups to achieve their goals directly using violence. Designing their attacks to produce panic and fear—to magnify the effect of the operations they can carry out—provides a way around these practical constraints. This is the basis for Brian Jenkins’ classic, and often cited, assessment that “terrorists want a lot of people watching, and not a lot of people dead” (Jenkins, 1987). The use of coercion and exploitation of the psychological impact of violent attack are defining characteristics of terrorism.⁵ Accordingly, the actual targets of terrorist acts extend well beyond the individuals or structures directly harmed. In the case of economic targeting, the idea is that introducing uncertainty through a credible threat of destruction or damage can be sufficient to inflict economic costs (or, stated alternatively, reduce economic well-being).

But recent, very large-scale terrorist operations—such as al Qaeda’s attack on the World Trade Center on September 11, 2001—have called parts of this traditional definition into question. The nature and scale of damages of the attack itself were great enough that it had

⁴ See, for example, discussion in *Al-Battar*, al Qaeda’s online biweekly training manual.

⁵ Other terrorist organizations have also engaged in economic targeting. Left-wing ideological groups in Europe, including the Red Brigade and the Red Army Faction, have targeted the private sector and businesspeople individually. The Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka targeted energy resources and the country’s financial center, Colombo.

⁶ Not all violent actions by terrorist groups are designed to achieve the group’s external goals. A large body of work on motivations for terrorism focuses on the organizational and psychological dynamics that can produce violent action which may or may not be directed at achieving particular instrumental goals. See Victoroff (2005) for a review.
an impact independent of the terror it produced: Its direct effects also contributed to achieving al Qaeda’s goals. The 9/11 attacks showed that a sufficiently large act of terrorism (coupled with ensuing cascading effects) can have significant consequences even for a large national economy.6

With both the traditional and the post-9/11 understandings of terrorism in mind, we define economic targeting as a terrorist group’s intent to inflict economic costs on a targeted state by doing one or both of two things:7

- threatening to destroy or damage property8 or harm people
- actually destroying or damaging property or harming people.

For a specific terrorist action, causing economic damage may be a group’s primary intent or may be only one of a range of goals the group has in mind.

**Two Types of Economic Targeting:**

**Episodic Terrorism Versus Terrorist Campaigns**

Terrorists have taken a variety of approaches to economic targeting. The 9/11 and PIRA attacks—both vivid examples of this type of terrorism—stand at two ends of a spectrum of possible activity:

- isolated, high-profile, high-impact attacks (9/11)
- campaigns of repeated, smaller-scale incidents (PIRA).9

An individual high-profile terrorist attack such as 9/11—to which we refer as episodic terrorism—occurs at a defined point in time. Attack planners design it to generate large economic costs. After the attack is carried out, its effects travel through an economy, producing additional costs, in some cases decaying and in others persisting over time.

---

6 These cases, in which an attack’s effects can achieve terrorists’ goals directly (i.e., in which violence itself is instrumental rather than coercive), blur one of the distinctions made between terrorism and other forms of targeted violence, such as state military action.

7 Our definition is similar to that used across the literature on this topic. See OECD (2004) for a particularly useful discussion.

8 We define property as “systems and assets, whether physical or virtual” (see Public Law 107-56). Assets also include productive capital and goods in inventory or pipeline.

9 In fact, these are two of four extreme cases: (1) high-frequency, low-intensity terrorism (campaign terrorism), (2) low-frequency, high-intensity terrorism (episodic terrorism), (3) low-frequency, low-intensity terrorism, and (4) high-frequency, high-intensity terrorism. Cases 3 and 4 are less relevant for policy consideration, however. In case 3, the economic impact would be small and therefore of much less concern. Case 4 is of limited probability given the capability constraints of non-state terrorist groups. It instead more closely resembles interstate war. If it did occur, it would demand of governments such drastic changes and measures that discussing its costs to the ex ante economy is not terribly meaningful.
In contrast, in an extended terrorist conflict such as PIRA’s—which we call campaign terrorism\textsuperscript{10}—the occurrence of each individual terrorist event and the costs it produces are less important than the expectation that the group will repeat the violence. Recurrent violence becomes a feature of the economic environment.\textsuperscript{11} In campaign terrorism, costs are designed to build up and compound over time, rather than stem from one specific attack.

These two types of economic targeting have very different profiles, both in the way individual costs accrue and the way the total cost tends to be distributed. But in both cases, the overall cost can be broken down into two main subcategories:

- costs caused by actual terrorist attacks
- costs generated by the perceived level of threat.

How much of the total outlay comes from attack costs versus from costs stemming from the perceived threat level differs markedly between episodic and campaign terrorism. Episodic terrorism has a large attack cost component, potentially less cost driven by threat; campaign terrorism is much more driven by costs from responses to threat than by attack costs. These individual costs also occur also in dissimilar time frames.

By comparing the 9/11 and PIRA attacks, we can readily observe differences in how costs mount and tend to be distributed in these two different forms of economic targeting. In practice, there is much grey area between the two extremes, and clearly distinguishing episodic from campaign terrorism usually requires the benefit of hindsight. A group that stages repeated attacks but very infrequently, for example, can be difficult to diagnose: Where its strategy falls on the spectrum between episodic and campaign terrorism will depend on perceptions of how frequently violence will be repeated. Other instances of economic targeting will similarly fall at different points between the two extremes.

**About This Report**

This report’s goals are as follows:

- to illustrate the potential economic effects of episodic versus campaign terrorism
- to inform policymakers about the full range of economic costs that may result from economic targeting—not all of which will occur with every event
- to explore the range of defensive measures that might be used to respond to this threat.

From the examples provided by 9/11 and the PIRA campaign, we draw key concepts useful for describing and anticipating the economic costs of other potential terrorist threats. To do so, we refer to analyses from existing literature on the topic, developing a framework that

\textsuperscript{10} Other examples of campaign terrorism include Palestinian terrorism aimed at Israel and the operations of the Basque group ETA (Euskadi Ta Askatasuna, or Basque Fatherland and Liberty) in Spain.

\textsuperscript{11} See Economic Analytical Unit (2004) for a similar discussion of the differences between terrorism as shock and terrorism as a means of creating a permanent change in economic conditions.
can capture both the acute effects of terrorist attacks and the longer-term effects of an ongoing threat of terrorism.\textsuperscript{12} Then, armed with the ability to anticipate costs and understand whence they come in different types of targeting, we explore the defensive approaches that might be implemented to reduce them.

\textsuperscript{12} We have not attempted to precisely assess and measure the economic consequences of particular terrorist events or terrorism overall, nor did we set out to estimate the economic costs and benefits of specific security and preparedness measures.
CHAPTER TWO

The 9/11 Attacks: The Economic Costs of High-Impact Terrorism

On September 11, 2001, operatives affiliated with al Qaeda hijacked four commercial airliners with the intent to use them as weapons in a larger terrorist attack operation. One of the airliners struck the Pentagon in Arlington, Virginia; a second, because of action taken by the passengers, crashed in southwestern Pennsylvania rather than striking its intended target; the other two struck the twin towers of the World Trade Center in New York City, the heart of the U.S. financial sector. The planes’ impact and the resulting fires led both towers of the World Trade Center to collapse. More than 2,900 individuals died in the attacks—more than the number killed in the attack on Pearl Harbor during World War II (National Commission on Terrorist Attacks upon the United States, 2004, pp. 1–2).

With the benefit of hindsight, the September 11 attacks represent an example of high-impact, episodic terrorism. Although it was far from clear in the immediate aftermath that this would be the case, similar attacks have fortunately not been repeated to date.¹ As a result, we can examine 9/11 to better understand the economic effects of a significant, but transitory, terrorist shock to an economy.

The Economic Effects of the September 11, 2001, Attacks

In terms of economic damage, perhaps most unprecedented about the 9/11 attacks was the scale of its direct costs. The expense of the physical destruction and subsequent cleanup efforts alone reached into the billions of dollars. Broader analyses of the attack costs have included, to varying extents, values for human lives lost, property loss, response and recovery costs, costs from injuries (psychological and physical due to both mechanical causes and hazardous exposures), temporary living assistance for displaced persons, impacts on businesses (including cascading effects from firms that closed, cut back, or reduced spending), and delays to travelers and commuters (Kingsbury, 2002).²

¹ Indeed, terrorist groups have incentives to give the impression of campaign-style operations both to bolster their apparent capability and sustain a single event’s effects over time.

² Some estimates also included tax revenues lost to the government, although “Fiscal impacts such as reduced tax revenues are represented in gross income losses, since taxes are transfers of income from taxpayers to government” (Kingsbury, 2002).
Emphasizing the difficulty in estimating cost impacts of such events, estimates of the attacks’ total direct and cascading costs have varied considerably but generally fall in the tens of billions of dollars. Attempts to estimate the attacks’ aggregate impacts by examining the country’s overall economic performance in their aftermath have sought to separate them from the effects of the general economic downturn under way at the time (see Makinen, 2002, for a discussion). Effects on specific industries—particularly aviation, given its direct connection to the attacks—have also been examined in detail:

September 11 resulted in both a negative transitory shock of over 30% and an ongoing negative demand shock amounting to 7.4% of pre-September 11 demand [for airline travel]. This ongoing demand shock has yet to dissipate [as of November 2003] and cannot be explained by economic, seasonal, or other factors. (Ito and Lee, 2005, p. 75)

As a result of the change in the perception of a terrorist threat, the U.S. government significantly increased expenditures on defense and homeland security activities. The U.S. Congressional Budget Office (CBO) estimated expenditures on homeland security specifically in fiscal year 2004 at $41 billion—“roughly double the amount allotted to those activities before September 11” (CBO, 2004).

Analyses have also assessed the costs of security for particular industries or potential targets. For example, security costs for the aviation industry (addressing federal government expenditures only) from 2002 to 2006 totaled $9.3 billion (Coughlin, Cohen, and Khan, 2002). RAND analyses have examined the costs and benefits of individual measures for enhancing aviation security, such as defenses against man-portable anti-aircraft missiles (Chow et al., 2005) and new baggage screening technologies (Shaver et al., 2004). These studies examined not only the direct costs of acquiring and maintaining such security investments, but also the indirect costs these measures have imposed on other groups, such as the traveling public.

Similarly, available data suggest that commercial firms modified security measures in response to the threat of terrorism. Fifty-three percent of the firms responding to a Council on Competitiveness survey (2002, p. 19) increased security spending between 2001 and 2002. A more extensive study by the Conference Board also indicated that about half of companies permanently increased security spending after 9/11, although the amount of the increase from firm to firm varied widely. Spending on insurance and risk management in particular increased markedly (Cavanagh, 2005; Czinkota and Knight, 2005). For the private sector, CBO estimated that security expenditures in 2002 stood at $20 billion (roughly 0.3 percent of GDP) and estimated a permanent reduction in total factor productivity of 0.03 percent going

---

3 For example, a RAND analysis of compensation after the attacks tabulated claims of approximately $38 billion (Dixon and Stern, 2004).

4 See also Blunk, Clark, and McGibany (2006).

5 Firms’ preparedness expenditures can also include other changes other than “traditional security choices” that require resources to implement (e.g., increasing backup or contingency capabilities, response activities, and distribution of activities across multiple sites). For example, a survey of corporate real estate managers after 9/11 indicated shifts in business opinions on topics such as the amount of public access allowed to buildings, planning for escape from buildings, backup telecommunication infrastructures, and information technology security (Laing, 2003).
The 9/11 attacks caused significant disruption in the nation’s financial sector, which affected the functioning of many critical markets and payment operations (reviewed in Lacker, 2004). These disruptions required the Federal Reserve to take action to ensure sufficient liquidity in the financial system. The shutdown of the U.S. air transportation system immediately after 9/11 had costly, acute effects on businesses, particularly on manufacturing firms that had transitioned to just-in-time delivery of intermediate goods (OECD, 2002, pp. 118, 128). Moreover, changes made to security that slow the delivery of goods or increase unpredictability in transport systems continue to produce costs over time (Brück, 2004, p. 110).

One estimate of the global welfare loss from the result of tighter security precautions post-9/11 on trade puts it at about $75 billion (Walkenhorst and Dihel, 2002). However, the actual effects could vary in different trade scenarios and among sectors, particularly affecting those whose products have comparatively low values to weight (Walkenhorst and Dihel, 2002). Other assessments of the impact of increased security in international trade estimated that measures (in 2002) could increase the ad valorem costs by 1 to 3 percent (OECD, 2002, p. 118).

Many businesses began to include resilience and robustness measures as part of their business planning after 2001 (Sheffi, 2001; Rice, 2003; OECD, 2003a, and references therein). For example, large U.S. firms were estimated to have increased their inventories to address the heightened uncertainty in transportation, potentially costing the U.S. economy between $50 billion and $80 billion in 2002 (OECD, 2003a, and references therein).

The change in perceived risk of terrorist attack also reportedly affected choices about where to locate business activities. Although U.S. firms operating overseas commonly took such risk considerations into account in deciding on locations, 9/11 reportedly led firms to begin to make similar assessments for domestic operations as well. Such considerations have reportedly affected firms’ decisions to agglomerate in specific areas (Czinkota and Knight, 2005; Rossi-Hansberg, 2004) and, as a result, have affected local economic geography. High-resolution models have examined the potential impact of such decisions on the structure of cities, labor rates demanded in risk areas, and rental rates (Rossi-Hansberg, 2004). The 9/11 attacks also influenced investment behavior and the willingness of individuals or firms to commit their resources to areas they perceived as higher risk. Investors from Middle Eastern nations, for example, reportedly pulled out significant sums of money from investments in

---

6 Responses of the Federal Reserve and of the payment system to 9/11 are discussed in Lacker (2004), Williamson (2004), and Lang (2001).
7 See also Brück (2004, p. 110).
8 Remarks of Jim Brooks, Vice President, Control Risks Group, Monterey, California, August 2005. Such decisions were driven by concerns that the attack was the beginning of a terrorist campaign rather than an isolated terrorist episode. This emphasizes the difficulty of identifying episodic versus campaign terrorism without the advantage of hindsight.
9 Abadie and Gardeazabal (2005) have estimated that a standard deviation increase in the risk of terrorism in a country “induces a fall in the net [foreign direct investment] position of about 5 percent of GDP.”
the United States after 9/11 for a variety of reasons, helping economies closer to home (Krane, 2005).

Though significant impacts on consumer attitudes and behavior were expected after such a major terrorist attack, consumers showed remarkable resilience in the face of terrorism. Indications of consumer confidence “maintained a fairly normal relationship to other economic indicators . . . [showing that] the decline of consumer confidence in the fourth quarter of 2001 was due mostly to weaker economic conditions in previous quarters and not to the September 11 attacks” (Garner, 2002, p. 19; OECD, 2002, p. 119). Consumer and even business behavior vis-à-vis the banking and financial sector was similar:

[O]ne might have expected the events of September 11 to generate anxiety among uninsured depositors and other uninsured bank creditors. In fact, while there was a blip in withdrawals from the banking system, it was very minor. Business customers who had lines of credit might also be expected to draw down existing lines before banks reassess their willingness to lend. Was there a huge rush to draw down lines of credit? While we did see some of that in industries most directly affected by the attacks, this again was a relatively minor event. The attacks of September 11 did not cause any significant financial panic among banks’ business customers. So the main story was that there was no story. (Lang, 2001, pp. 361–362)

But the attacks hit specific industries, on the other hand, very hard. The demand for airline travel dropped significantly, at great cost to the aviation sector (Ito and Lee, 2005; Blunk, Clark, and McGibany, 2006). Tourism also suffered: Tourist arrivals to the United States declined after the attacks (Australian Department of Foreign Affairs and Trade, 2004). The Washington, D.C., area, site of the Pentagon attacks experienced impacts on tourism after 9/11, with further effects on tourist demand when the terrorist alert level was raised (Ip, 2004).

The damage to certain industries may have had indirect economic costs as well. For example, in the period after 9/11, road fatalities increased significantly, likely as a result of the diversion of travelers from airlines to the nation’s roadways (Blalock, Kadiyali, and Simon, 2005, p. 20).

Discussion

The 9/11 attacks acted as a “shock” to the U.S. economy, producing “waves” that moved out over time through various economic sectors. How the economy absorbed and addressed the shock effects determined the resulting economic costs. In this sort of episodic, high-impact terrorism, the costs of an attack itself are high because of the sheer scale of the event. These costs contribute significantly to the total economic impact. Many of these costs occur during the attack itself. Others may be temporary—economic losses due to a short-term delay in the

---

10 See also Enz and Canina (2002) and Stafford, Yu, and Armoo (2002).
11 See also the analysis in Gigerenzer (2006).
delivery of goods, for example. Still others can be enduring, such as the destruction of trans-
portation capital that damages the ability to deliver goods over a longer time horizon. Though
the impact of such direct costs may be large immediately after an attack, as they are resolved
over time, their contribution to the total economic cost drops off.

High-impact shocks like 9/11 can affect prices for goods and services (Thissen, 2004)
and require large outlays to remediate or compensate for damages. Government and businesses
may divert resources to security. Consumer and investor behavior may also change in ways that
lead to considerable costs. The extent of expenditures on security and preparedness measures,
as well as the losses due to changes in behavior, will be determined by the level of threat that
government, businesses, and individuals perceive after the event and for how long the percep-
tion of elevated threat is sustained. Whatever costs are incurred after an attack from changes
in behavior or expenditures on additional security and preparedness, if no additional attacks
are assumed, the economic effects may decay and disappear as the perception of threat dis-
sipates. But if the fear of repeat attacks persists—i.e., there is concern that the event is not, in
fact, episodic terrorism, but one event in a campaign—then increased security spending and
effects on behavior will remain cost drivers for a longer period.

To understand the full economic consequences of a high-impact, episodic attack, one
must account for both the damage from the attack itself and how any additional costs may add
up over time. This requires assessing both cascading effects and changes in behavior that will
continue to produce a stream of costs as the economy reacts to the initial shock.

A terrorist group that opts to pursue the high-impact approach to economic targeting must
design an attack that will maximize direct costs. A variety of other hypothetical attack sce-
narios would achieve this objective. Nuclear events; large-scale bombings of dense target areas
(e.g., central business districts or concentrated business centers); and major chemical, biologi-
cal, and radiological attacks define the upper range of this group, given that they would affect
large areas and populations and require massive response and recovery expenditures (Hyams,
Murphy, and Wessely, 2002). Terrorists might also use infrastructure assets in violent action
ranging from essentially conventional (e.g., the use of airliners in the 9/11 attacks as vehicle
bombs) to large-scale, unconventional offensive weapons (e.g., the use of stored chemical stocks
at industrial sites or in the transportation infrastructure.) In such cases, costs would reason-
ably resemble those seen for large-scale natural disasters (see, for example, OECD, 2003b).13

12 Concerns about risks of terrorism can produce demands for security and preparedness expenditures by other actors
within the economy. Demands by individuals can influence security choices by firms and the government, with such
demands differing from person to person. For example, how people reacted to 9/11 (e.g., anger versus sadness) shaped what
they saw as the appropriate policy response (Sadler et al., 2005). The tendency to increase security spending will certainly
differ among industries and among firms within a single industry, and risk concerns may also result in a firm calling for
additional national spending on security activities. In addition, because of externalities in systems in which individual
firms’ security choices affect the choices of all, incentives for investment in security can be significantly shifted by general
trends in other firms’ behavior (Coughlin, Cohen, and Khan, 2002; Heal and Kunreuther, 2005; Kunreuther and Heal,
2003).

13 Because natural disasters can generate similar shocks to economic systems and infrastructures, researchers have drawn
on experience with those events to inform estimates of the potential impacts of large terrorist attacks. See National Research
Council (1999) for a review.
Researchers have estimated the cost of direct damages to lives and property, the disruption to trade, and the cascading effects on industries for several such high-impact scenarios:

- For every 100,000 individuals exposed in a successful, large-scale, biological attack, costs would reach the hundreds of millions to tens of billions of dollars (Kaufmann, Maltzer, and Schmid, 1997).
- An attack involving nuclear explosions in large cities with major port facilities would cost hundreds of billions to trillions of dollars (Abt, 2003).
- A loss of approximately $60 billion would result if radiological weapons were used to close shipping facilities (Fields, 2002).

Because the effectiveness of economic attacks using this approach depends on their scale, it is vital to be able to understand just how high their potential costs can reach and how they will accrue. But as the example of 9/11 demonstrated, the complexity of modern economies makes this sort of detailed and accurate understanding quite difficult. Much current research focuses on developing tools to help assess both those interconnections among sectors of the economy that could magnify the effects of such attacks and the adaptability and resilience of businesses and other elements of the economy that could help to dampen them out.

---

14 A growing literature examines terrorist attacks through sophisticated, agent-based models (for example, the research program under way at Sandia National Laboratories and the National Infrastructure Simulation and Analysis Center [Backus, 2005; Sprigg, 2004], input/output models [Santos and Haimes, 2004], and other models). Such models allow for much broader study and hypothesis-testing of the effects of various terrorist attacks on public and organizational behavior. In addition, they provide ways to model the potential cascading effects of attacks within sectors and among structures that can take place because of the interconnections among infrastructures and economic systems. Santos and Haimes’ (2004) sophisticated input/output framework uses the full 483 North American Industry Classification System (NAICS) industries and the interconnections among them to examine the economic effects that reductions in demand in specific sectors can have on the economy as a whole. Increasingly sophisticated models of economic activities and specific infrastructure systems are also rapidly improving the ability to assess the costs of attacks on transportation (Haimes, undated; Bae, Blain, and Bassok, 2005), electrical power (Chang, McDaniels, and Reed, 2005; Lave et al., 2004; Rose, Oladosu, and Liao, 2005; ICIS, 2005; Amin and Gelling, 2005), shipping (Gordon et al., 2005; Park et al., 2006), and tourism (Richardson et al., 2005).

15 A study of the 2002 West Coast port labor dispute, which shut down multiple major ports for 10 days, suggested that many calculations of the costs of major economic disruptions overestimate their impact on the national economy (Hall, 2004). Most impact studies of the 2002 dispute, the resulting article claimed, either assumed the complete loss of the economic value of goods held back on ships, ignored the role of inventories in stabilizing other sectors, or ignored the potential ability of alternative—though admittedly higher-cost—transport modes to compensate. By making such assumptions, researchers failed to account for an economy’s capacity to adapt to such crises. More sophisticated models make it possible to assess the adaptability of economies in the face of large shocks. Studies using these models have determined that estimates of economic costs that do not include firms’ ability to substitute inputs, seek out new sources, and shift production activities in time can go unrealistically high. One analysis, for example, of the resilience of businesses to electricity disruptions estimated that adaptive behaviors can reduce the total net costs of incidents that cut off electricity service by between 50 and 95 percent (Rose, 2005).
PIRA waged a campaign of violence against the UK government between 1969 until a cease-fire in the mid-1990s. Recently, with the reported decommissioning of its arsenal, the group’s terrorist activities appear to have come to an end. PIRA conducted operations mainly in Northern Ireland and on the British mainland, with several forays into other countries. The group used the Republic of Ireland heavily for logistical activities and sanctuary but limited its violent activities in that country.

PIRA featured economic targeting prominently in statements of its strategic goals (Rogers, 2000). For example, the second goal on a list included in PIRA’s policy and training manual was “[a] bombing campaign aimed at making the enemy’s financial interest in our country unprofitable, while at the same time curbing long term financial investment in our country” (quoted in Coogan, 1993, p. 420). PIRA carried out a range of operations intended to damage the economies of Great Britain and Northern Ireland and influence economic decisionmaking:

- attacks and hoaxes aimed at transportation networks, energy infrastructures, central business districts, and financial institutions
- incendiary and bomb attacks on commercial establishments (e.g., retail stores, restaurants, hotels)
- assassinations of business leaders.

The violence in Northern Ireland took a sizable human toll, as a result both of PIRA’s operations and of those of sympathetic and opposing terrorist organizations. More than 3,300 people died and 48,000 were injured. Attacks on the British mainland and elsewhere added more injuries and fatalities to the total. Northern Ireland is relatively small, with an average

---

1 Specific targets included airports, trains, ferries, and surface transportation.
2 Specific targets included electrical substations, pylons, transmission lines, coal ships, refineries, and gas plants.
3 A variety of other terrorist groups operated in Northern Ireland during the same period as PIRA. Other Republican groups used terrorism to pursue goals similar to PIRA’s, including the unification of Northern Ireland with the Republic of Ireland. A number of Loyalist groups opposed unification with the Republic and used terrorist violence to prevent it. Sectarian differences between the Republicans, drawn largely from the Catholic population, and the Loyalists, who were largely Protestant, also drove the conflict.
4 Data from the Police Service of Northern Ireland (2005).
5 Data from the Police Service of Northern Ireland (2005).
population during the period of approximately 1.5 million people. In a larger and more populous country like the United States, a similar density of violence would have involved hundreds of thousands of people killed (New Ireland Forum, 1983, p. 5).

PIRA’s approach to economic targeting lies at the other end of the spectrum from al Qaeda’s in the 9/11 attacks. Although some of its individual operations were, indeed, large-scale attacks that produced major damage, most were much smaller. The bulk of their total economic costs came from their cumulative effect over time and their influence on Northern Ireland’s economic environment.

The Economic Effects of the PIRA Terrorist Campaign

For assessing their economic effects, PIRA’s activities can be viewed as falling into two broad categories: (1) its attacks in Northern Ireland—primarily small operations whose effects added up over time—and (2) its operations on the British mainland, which were less frequent but occasionally much larger-scale attacks. The differences between these two related campaigns produced somewhat different economic outcomes.

PIRA Operations in Northern Ireland

PIRA conducted a wide variety of terrorist operations in Northern Ireland. It also kept the number of attacks high, frequently staging hundreds or even thousands per year. Most common were shootings and bombings, though, over time, the group utilized many more sophisticated techniques, such as mortars. The scale of its attacks varied from a single shot intended to injure or kill one individual to car bombings in commercial centers that could produce large amounts of physical damage and large numbers of human casualties. Targets ranged from UK military patrols and members of law enforcement to commercial and infrastructure installations.

The variety of PIRA’s activities meant that the economic costs that each attack generated varied greatly: A single rifle shot that missed its target might produce no direct costs but still contribute to indirect costs stemming from the overall environment of fear and insecurity. A car bombing or major incendiary attack might produce significant economic costs from physical damage, injuries, or fatalities, as well as heightening the population’s perception of risk.

As a matter of public policy, the UK government paid compensation to individuals injured (or to the families of those killed) and for property damaged. As a result, compensation expenses can provide a measure of one part of the conflict’s direct costs. By the end of March 1982, approximately £1,010 million (in 1982 prices) had been paid as a result of

---

6 During the conflict, two major assessments were made of its costs: The Cost of Violence Arising from the Northern Ireland Crisis Since 1969 (by the New Ireland Forum, published in 1983) and an extension of that analysis included in the public record of debate of the Dáil Éireann titled “Written Answers: Exchequer Cost of Northern Ireland Violence” (Reynolds, 1990). Because those sources focus on the costs of the conflict in Northern Ireland (and, to a lesser extent, the Republic of Ireland), they do not describe the costs for attacks on the British mainland or fully capture the extensive security measures put in place in response. This section summarizes data from these two analyses.

7 Available statistics on the conflict include attacks by all terrorist organizations active in Northern Ireland (Police Service of Northern Ireland, 2007).
the conflict in the North (New Ireland Forum, 1983, pp. 11–12, 25). Values for 1983–1989 (also calculated in 1982 prices) have been reported to have been an additional £182 million (Reynolds, 1990). In the Republic of Ireland, compensation costs were a more modest total of £31 million in 1982 prices. This is not surprising, as PIRA did not routinely carry out offensive operations in the Republic.

In response to the violence, the UK government committed resources to security efforts involving both law enforcement and military organizations. Costs included the expenses of security activities themselves and also of protecting the security forces, whom PIRA frequently targeted. For example, significant amounts of money were spent to “mortar proof” police bases in Northern Ireland to harden them against attack. Over the course of the conflict, the costs of security measures added up. The total cost of extra security for the years 1969–1989 (in 1982 prices) was £9,826 million (Table 3.1) in both Northern Ireland and the Republic of Ireland. Expenditures also increased on prisons to hold those individuals incarcerated as a result of security activities. In 1983 (the only year for which data are available), this resulted in a cost of approximately £56 million (New Ireland Forum, 1983, p. 14).

Table 3.1
Security Costs in the Northern Ireland Conflict, 1969–1989

<table>
<thead>
<tr>
<th>Period</th>
<th>Northern Ireland</th>
<th>Republic of Ireland</th>
<th>Overall Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1969–1982</td>
<td>4,245</td>
<td>990</td>
<td>5,235</td>
</tr>
<tr>
<td>1982–1989</td>
<td>3,859</td>
<td>732</td>
<td>4,591</td>
</tr>
<tr>
<td>Total</td>
<td>8,104</td>
<td>1,722</td>
<td>9,826</td>
</tr>
</tbody>
</table>


NOTE: Extra security costs for Northern Ireland include the cost of keeping the British army deployed in the region and of private security. Figures are in 1982 prices in millions of pounds Sterling.

8 Approximately $2.5 billion (in 2004 dollars, based on an average exchange rate in 1982 and U.S. OMB GDP deflators).
11 See Brian A. Jackson, Chalk, et al. (2007) for a description of the security measures implemented in response to PIRA’s campaign.
12 “In 1971 the Crossmaglen RUC [police] barracks in South Armagh was a brick-built house with wire mesh on the windows and nothing more. By 1997 it had walls 7ft thick and a top floor kept empty as a unit of ‘space armour’” (security expert quoted in Geraghty, 2000a, p. 193).
Private-sector organizations also spent considerable amounts on security in response to the conflict:

[A] bombing campaign leads to a long-term increase in overheads as companies maintain higher levels of security, indeed it tends to boost the development of costly disaster recovery industry in its own right. . . . By late 1993, disaster recovery in Britain was reported to be an industry worth £150 million per annum and growing by 25 per cent per year. Much of this expenditure was in response to PIRA activities, most of it incurred by larger business organisations. (Rogers, 2000)\(^{14}\)

The UK government incurred related costs, providing an “official premium . . . to hotels and other commercial undertakings towards the cost of maintaining security staff” in Northern Ireland. Between 1975 and 1982, this came to approximately £50 million in 1982 prices (New Ireland Forum, 1983, pp. 13, 25). Firms also paid other direct costs associated with the violence, including risk management, as well as less tangible effects on economic performance because “attacks impair[ed] the morale and commercial efficiency of organisations directly affected” (Rogers, 2000).

Beyond the direct costs, the violent environment imposed a range of opportunity costs on firms operating in Northern Ireland. One case study characterizes the economic impacts of damage PIRA did to a critical chokepoint in an electrical system:

Because of the small and isolated nature of both electricity systems in the North and the South, generating costs are substantially higher than in other European countries. It is accepted that the linking of both electricity systems should confer economic benefits in terms of: (1) capital savings because co-ordinated planning could ensure that surplus reserve generating capacity needs would be lower; (2) savings in operating costs because of lower ‘spinning reserve’ requirements (power stations on standby); (3) economies resulting from energy trading to mutual advantage. An inter-connector between both systems was commissioned in 1970. During the 13 years of its existence it has only been operational for 24 per cent owing to bomb damage on six occasions and has not been operational at all since 1975. Intimidation of repair teams has frustrated efforts to restore the interconnector. (New Ireland Forum, 1983, pp. 23–24)

Total economic losses resulting from PIRA operations targeting the interconnector were estimated at £190 million in 1982 prices (New Ireland Forum, 1983, p. 25).

The increasing demand for security in the region resulted in shifts in employment in the conflict zone. In 1982, the UK government estimated that more than 12,000 new jobs in security had been created in Northern Ireland since 1969, compared with an overall estimated gross loss in the region of 39,000 jobs (New Ireland Forum, 1983, p. 19, and references therein). Although the increase in security jobs reduced the overall job losses, the growth in the security sector represented a significant diversion of resources from productive employment in a region with a total population of approximately 1.5 million. A separate 1984 assessment of

\(^{14}\) This source does not separate expenditures in Northern Ireland from those in the UK overall.
unemployment in Northern Ireland estimated that there were 122,000 people without jobs, corresponding to between 25 and 33 percent unemployment.15

Northern Ireland’s tourist industry was significantly affected, with a clear correlation between the intensity of violence and drops in tourism (Lennon, 1995; New Ireland Forum, 1983). Emigration was another costly outcome, as PIRA’s campaign produced large population shifts:

[I]n Belfast alone over 60,000 people moved residence, largely because of violence and intimidation. . . . Between 1971 and 1981 the North, by contrast with the South (which experienced an annual net immigration of 10,000 annually), had a net outward emigration of about 8,000 per annum. (New Ireland Forum, 1983, pp. 7–8)

Many of the people leaving were young and left for education and never returned. Efforts have been made to calculate the overall net economic impact of PIRA’s operations on the region, even though separating out direct causal connections between violence and macroeconomic performance is challenging:

Although it is certain that the violence has damaged [Northern Ireland’s] economic performance, it is difficult to quantify precisely the extent to which the violence, as distinct from other significant factors, affected the North’s economy. . . . An examination of the variation in performance of the North’s economy in relation to that of Britain and some of its regions helps to distinguish between the influence of violence and other negative factors on the decline in output. . . . In the 10 years prior to when the violence began in 1969 average annual GDP growth in the North was approximately 40 percent above that in Britain. However, between 1969 and 1982, despite substantial growth in transfers from Britain, average annual GDP growth in the North was only 40 percent that of Britain. (New Ireland Forum, 1983, p. 18, emphasis in original)

The New Ireland Forum estimated an average annual loss of real GDP growth from the violence (expected minus observed growth rates) of 1.4 percent per year. This results in a total estimated economic loss for the period 1969–1982 of £3,490 million in 1982 prices (New Ireland Forum, 1983, pp. 18–19).16 The overall total of the economic estimates available from the New Ireland Forum report (1983) and subsequent updated estimates (Reynolds, 1990) for expenditures, damages, and other economic costs for the conflict over this period is £14.8 billion in 1982 prices.

PIRA Operations on the UK Mainland
PIRA staged attacks outside Northern Ireland, particularly on the UK mainland, much less frequently than within that region. Best estimates of the number of operations that the group carried out in England are in the hundreds (Brian A. Jackson, Baker, et al., 2005b). These


16 Approximately $8.9 billion (in 2004 dollars, based on an average exchange rate in 1982 and U.S. OMB GDP deflators).
operations included letter bombs targeting individuals, explosives planted in public areas like the London Underground, and very large-scale vehicle bombings designed to cause massive damages.

Much less quantitative data on the economic effects of the PIRA England campaign overall is available. The economic effects of smaller-scale events were produced primarily by the disruption and fear they generated. For example, the group’s attacks on transportation infrastructures led to significant disruptions to traffic flow, causing major effects on rail and surface transport (Rogers, 2000). But its large-scale bombing operations, such as those it staged in London’s financial district, produced damages in the millions of pounds, causing more than £1 billion in damages on multiple occasions:

Prior to the 9/11 attacks, the IRA’s bombing of Bishopsgate in the City of London on April 1993, which had an insured cost of $907 million, had been the world’s most expensive terrorist attack. The full cost of the Bishopsgate attack was much higher as it inflicted extensive damage to Liverpool Street station, caused the closure of parts of the City for several days and resulted in the demolition of a number of office buildings that had been rendered structurally unsound. (London Chamber of Commerce and Industry, 2005, pp. 8–9)

In response to PIRA’s attacks in England, significant security measures were implemented to combat the terrorist activity. Law enforcement and intelligence organizations increased their activity. Both the UK government and the private sector also invested substantially in building physical and technological defenses. What became known as the “Ring of Steel” was put in place around the London financial district, the target of some of PIRA’s most costly massive bombing operations: The area was closed to most vehicular traffic, and a huge surveillance and guard force routinely searched individuals and vehicles. Protective measures also surrounded other prominent targets (Coaffee, 2004). While accurate estimates of the costs of these measures are not available, the outlay they required contributed to the conflict’s economic costs.

Like in Northern Ireland, PIRA attacks on the British mainland—in London in particular—affected tourist bookings (Rogers, 2000; New Ireland Forum, 1983). There was also concern that large foreign businesses would similarly “substitute other locations” for London to insulate themselves from the risk of violence:

[T]he damage caused by a bombing campaign and its aftermath can have a substantial effect on the status of a major business centre, especially in relation to its competitiveness with other centres. For the City of London in the early 1990s, the problem was not so

---

17 “It is hard to gauge the economic impact of the IRA’s early offensive operations in the UK because these operations were waged over a very long period, were directed against a wide variety of targets, were conducted with varying degrees of ‘success’ by the terrorists and varied greatly in terms of the tempo and intensity of activity. They were also conducted against the backdrop of considerable economic and political turbulence at home and abroad, typified by escalating industrial unrest, the oil crisis and the three-day week” (London Chamber of Commerce and Industry, 2005, p. 8).

18 See, for example, Geraghty (2000a, 2000b) for descriptions of damages from major PIRA operations on the UK mainland, and Coaffee (2004) for an overview of security measures taken in response.

19 See Brian A. Jackson, Chalk, et al. (2007) for a description of the security measures implemented in response to PIRA’s campaign.
much in relation to major British financial institutions, as most of them operate in London for a variety of commercial reasons which make relocation difficult. They are, in a sense, a captive market by virtue of the location of their own markets. Far more problematic was the status of overseas financial institutions located in London. Competition with other European financial centres, especially Frankfurt, was intense, and the risk of major bomb attacks would be far more likely to affect the choice of location with feasible alternatives being available. (Rogers, 2000)

This concern led to a “pronounced tendency on the part of the relevant authorities [in England] to minimize the effects [of economically targeted terrorism] in public” (Rogers, 2000, p. 6) both to deter attacks and reduce the potential of the additional costs such decisions would cause.

Discussion

The repeated attacks that PIRA staged as part of its extended campaign of economic targeting became an integral part of the economic environments of the British mainland and Northern Ireland. In contrast to single episodic terrorist events, in which concepts of short- and longer-term costs have meaning, during campaign terrorism, the resulting costs are not so easily broken down into such clean time frames. In a long-term terrorist campaign, individual attack costs are usually low, making the economic effect of any isolated event small. But the costs of many small events can accumulate appreciably over time, producing a much larger total cost.20

PIRA’s operations were not solely made up of small attacks. Operations such as the bombing at Bishopsgate produced significant damages. But questions have been raised about how much independent economic effect such large events exert on their own. Regarding Bishopsgate, the London Chamber of Commerce and Industry concluded, “[T]he economic effect of this considerable disruption was minimal. The economy continued to recover during the second quarter of 1993 just as it had previously and the Bank of England did not refer to the incident in its May 1993 economic assessment” (2005, p. 9). This suggests that, although events like Bishopsgate stand out for their scale, it is not inappropriate to examine them in the context of the total terrorist campaign of which they are a part.

The central characteristic of campaign terrorism is that repeat attacks of some type are almost certain. This creates a perception of an ongoing threat that influences government, business, and individual behavior in ways qualitatively different from that in episodic, high-impact terrorism. For example, it becomes very common for governments to make longer-term commitments to expenditures on security and for a continuously elevated perception of risk.

---

20 Similar analyses have been done of the Basque terrorist group ETA in Spain and violence in Latin America (in particular, between the Revolutionary Armed Forces of Colombia [Fuerzas Armadas Revolucionarias de Colombia, or FARC] and the Colombian government).
among individuals and firms to affect economic activity.\textsuperscript{21} Indeed, available data on PIRA's operations indicate that the bulk of the overall cost of this type of economic targeting comes from the combination of ongoing outlays on security and preparedness measures and costs arising from behavioral changes over long periods of time.

Analyzing the aggregate performance of an economy overall is one way to attempt to account for the drag on economic performance caused by changes in behavior made in response to risk, direct expenditures on security measures, and the so-called “terrorist taxes” produced indirectly by security (e.g., delay of individuals and shipments due to searches or other measures).\textsuperscript{22} Branching out from the example of Northern Ireland, analyses have been done of the macroeconomic, sectoral, security, and other costs imposed by ongoing terrorist campaigns (see, for example, Abadie and Gardeazabal, 2003; Gupta et al., 2004).

Efforts aimed at fully capturing the effects of campaign terrorism on national economies have assessed those changes in GDP that can be linked to violence levels. Some such efforts have compared different nations, seeking to connect differences in economic performance to different violence levels. Results of such analyses have been mixed. Some studies see limited or no effects of terrorism on economic growth (Tavares, 2004, p. 1057; Blomberg, Hess, and Orphanides, 2004). Others find connections between instability and violence and differences in performance (reviewed in Abadie and Gardeazabal, 2003).\textsuperscript{23} A study of the effect of long-term violence on the economies of Latin American nations, for example, estimated reductions in GDP of approximately 14 percent and ranging from approximately 5 to 25 percent for individual countries (Londoño de la Cuesta and Guerrero, 2000).

But to make these determinations accurately, it is necessary to estimate “what would have happened” economically in the absence of violence, which is difficult. One study examining the effects of Basque terrorism in Spain, another example of a long-term terrorist campaign, attempted to address this problem by comparing the economic performance of areas of the country affected by terrorism with a control region without violence: “After the outbreak of terrorism in the late 1960s, per capita GDP in the Basque Country declined about 10 percentage points relative to a synthetic control region without terrorism” (Abadie and Gardeazabal, 2003).

\textsuperscript{21} The Economic Analytical Unit in the Australian Department of Foreign Affairs and Trade simulated the GDP impacts of the combined effect of a reduction in total factor productivity (from diversion of resources to security) and investors’ perceptions of equity risk. In its simulations, the combination of a 0.3 percent permanent decline in total factor productivity and a persistent 1 percent increase in investors’ risk premiums result in a reduction of U.S. GDP of approximately 2 percent. Impacts on individual nations differed considerably, depending on their economies’ reliance on both trade and foreign direct investment (FDI), both of which are adversely affected by the risk of terrorism (Australian Department of Foreign Affairs and Trade, 2004, pp. 11–12). Penm, Buetre, and Tran (2004) simulated the effects of an across-the-board 0.5 percent reduction in primary-factor productivity as a result of the diversion of resources to security expenditures.

\textsuperscript{22} See New Ireland Forum (1983), Chow et al. (2005), Shaver et al. (2004), OECD (2003a), and Hobijn (2002).

\textsuperscript{23} One issue raised about aggregate assessments of economic performance during periods of terrorist violence involves the complications associated with “counting” expenditures for security and other responses to the terrorist threat as part of a region’s economic output. Such economic activity, which would not occur in the absence of terrorism, is, in some ways, “artificial” and can apparently compensate for some of the reductions in economic activity caused by the violence (New Ireland Forum, 1983, p. 18).
Additional studies have assessed the effects of terrorism on individual industry sectors such as airlines (Ito and Lee, 2005) and tourism (Enders, Sandler, and Parise, 1992; Drakos and Kutan, 2003; Fleischer and Buccola, 2002). Similar approaches have been applied to other elements of economic relationships between nations, including the effects of long-term terrorism and violence on trade flows (Nitsch and Schumacher, 2004; Walkenhorst and Dihel, 2002) and FDI (Enders and Sandler, 1996; Abadie and Gardeazabal, 2005). In these cases, the ability of businesses and individuals to “go elsewhere,” whether for travel, trade, or investment, magnifies the economic costs of terrorist violence.\(^{24}\)

Because of the differences between the circumstances of the United States and areas with available data on the economic impacts of extended terrorist campaigns, analogies about potential effects should a similar campaign occur in the United States must be tentative. But assuming that the costs were proportional, even the lower-bound estimates of the percentage effect of a persistently violent environment on a nation’s GDP would correspond to large absolute amounts of money, given the scale of the U.S. economy.\(^{25}\) The case of Northern Ireland clearly demonstrates that economic costs can add up over time during a sustained campaign, producing significant total damages even in areas much smaller and less populous than the United States.

---

\(^{24}\) Penm, Buetre, and Tran (2004) simulate the effects of terrorism in a specific region, showing both capital flight and diversion of international trade from the affected area.

\(^{25}\) But alternatively, the economy’s scale could also lead to differences in effect, limiting the utility of such generalizations. For instance, a larger economy might provide a more substantial buffer against the effects of violence, leading to a less-than-proportional impact.
As the 9/11 attacks and PIRA’s nearly 30-year terrorist campaign show, economic targeting can produce a wide variety of costs, with total damages accruing in different ways, depending on the approach a terrorist group takes. These two examples provide an excellent starting point for looking more comprehensively and systematically at the full range of potential costs that economic targeting can generate. All of these costs, as well as how they accrue and how they can influence each other, need to be considered when assessing the total impact that a terrorist group may have on an economy. In this chapter, we present a framework that policymakers can use to make this kind of comprehensive assessment. The understanding it can provide of any given instance of economic targeting will lay the groundwork for decisions about what countermeasures might be best taken to prevent costs altogether or keep them as low as possible.

**Economically Targeted Terrorism Generates Three Types of Costs**

The costs of economic targeting can be divided into three classes:

- the costs of an attack itself
- the costs of implementing security and preparedness measures in anticipation of future attacks
- the costs resulting from changes in behavior due to the perception of the threat of future attacks.\(^1\)

Within each category, one needs to look at government, businesses, and individuals respectively for how much each contributes to the total costs of the terrorist activity.\(^2\)

---

\(^1\) Other authors have categorized the economic costs of terrorist attacks differently. See Brück (2005) for a somewhat different breakdown.

\(^2\) The fact that the government must raise money for its expenditures on security and preparedness measures through taxes creates possible distortions that will affect the real cost of these measures. In the basic framework outlined in Figure S.1 in the summary, we have considered expenditures by any party within the economy equivalent. Raising of revenue through taxation will produce shifts in economic decisionmaking by other parties within the economy that could increase the actual costs of these measures. As a result, rather than government, business, and individual expenditures being equivalent, implementation of preparedness and response measures by specific parties may produce efficiency gains. However, differences between private incentives associated with specific approaches to responding to terrorism risks and broader national benefits
Attack Costs

Attack costs occur during a terrorist attack and can continue to accrue in its immediate aftermath. These costs include

- damage to structures or other capital
- costs from individuals killed (including the loss of productive capacity)
- costs from injuries to individuals (including direct costs from injury, such as physiological and psychological treatment costs and losses in productivity or income resulting from disability)
- cascading effects within and among sectors from damages that affect other firms’ operations.

Attack costs can shrink a national economy, reduce its productive capacity, and put a drain on financial resources when money intended for other uses must be diverted to fix damages.

Security and Preparedness Costs

Security and preparedness costs accrue as governments, businesses, and individuals put measures in place to address any further terrorist threat following one or more attacks (Alexander, 2004). These costs include

- expenditures for security, response, and recovery measures
- indirect costs of those measures (e.g., increased wait times from security searches, inefficiencies in transport or supply chains).

---

3 Our category of attack costs includes outcomes that other authors have separated into direct and indirect effects of terrorism. We grouped costs in this way in part because of difficulties in consistently distinguishing between direct and indirect costs across a wide range of scenarios. Although the difference might be clear in a conventional terrorist attack on a defined site, it may be much more difficult to identify in attacks with unconventional weapons or strikes on networked systems such as water, power, or agriculture. We are aware that the difference between the two can be critical at times. For example, some insurance policies cover only “direct results of peril not excluded,” declining to cover any effects deemed “indirect” (Kunreuther and Michel-Kerjan, 2004).

4 See the discussion in Saxton (2002a).

5 “The indications are that the security industry [defined as ‘the aggregation of hundreds of thousands of businesses and individuals whose aim is to sell safety from malevolent acts threatening life, property and other assets, and information’ (Stevens, 2004a, p. 8)] is emerging as a big player in the economy, and expanding. Available estimates put the private security industry’s turnover at between USD 100 billion and USD 120 billion worldwide. The United States accounts for the largest share, although other OECD countries have sizeable security industries as well. . . . While there is little evidence within the industry of a major upsurge in spending on security since September 11, 2002, longer-term data suggest healthy growth in turnover in the order of 7–8% annually, easily outstripping average annual economic growth rates” (Stevens, 2004a, p. 9).
These costs consume financial resources that might be used for other purposes and divert resources from productive to unproductive use within an economy. Attempting to generate security and preparedness costs could be one element of a terrorist strategy to target a nation’s economy.

**Behavioral Change Costs**

Behavioral change costs result when individuals, firms, or the government alter their normal behavior in response to the threat of terrorism. These costs can include:

- reductions in demand because of fear or uncertainty
- changes in demand due to the behavior of financial markets or changes in the value of assets
- shifts in investment behaviors resulting from changed perceptions of risk that hurt the economy’s productive capacity
- additional or second-order economic costs produced by the shift in activity resulting from terrorism.

Each of these three classes of costs can accrue differently for government, businesses, and individuals. For example, expenditures on security and preparedness will be quite different for each of these parties. Table 4.1 provides examples of specific costs within each category.

---


7 For example, including expenditures on security efforts in aggregate economic accounts like GDP effectively offsets some of the economic costs of terrorism with the expenditures made in response to the threat.

8 Some security measures produce benefits that go beyond terrorism (e.g. crime prevention). These benefits may serve to reduce the effective costs of security and preparedness for terrorism. Information on those benefits of security expenditures not related to terrorism is less readily available than estimates of the costs of the security systems themselves.

9 For a recent discussion, see Neumann and Smith (2005).

10 Demand may be reduced in some areas but substituted in others. Frey, Luechinger, and Stutzer (2004, p. 7) cite the tourist industry as an example.

11 It is easier to understand the effect of the fear of potential terrorist threats on some sectors than on others. The reduced demand for air travel after the 9/11 attacks is easy to understand. In other cases, the behavioral change costs produced may be related simply to the risk environment and judgments about how that environment will affect demand for goods or services that an industry produces.

12 Note that these costs are not necessarily simply additive, as they may manifest differently over time and have different consequences on individuals versus firms versus government.
Understanding What Determines the Economic Costs of Terrorism: What Factors Drive Increases in Costs?

To provide a basis for defensive planning, we must understand what factors drive the costs of economic targeting higher. Drawing on the examples of the 9/11 and PIRA cases and on the broader literature on terrorism, we could construct a simplified picture in which two main drivers shape the total costs of terrorism:

- a terrorist group’s desire to maximize attack costs and its ability to use particular attack modes or exploit key vulnerabilities to do so
- the perception of government, businesses, or individuals that the risk of terrorism is high, producing both demand for security and preparedness expenditures and costs arising from behavioral changes.

The First Main Driver of Economic Costs: A Terrorist Group’s Ambition to Stage a Large-Scale, High-Cost Attack

Attack costs are purely incident-driven: The adversary’s desire to inflict economic harm, its choice of tactics and target, and the vulnerability of the target shapes these costs (Figure 4.1). They are therefore largely determined by the attackers’ decisions. To estimate these costs, analysts must anticipate a terrorist group’s operational decisionmaking: What kind of attack the

---

13 Additional costs and their drivers will be added to Figure 4.1 in later sections of this chapter to complete the framework.
Figure 4.1
Drivers of Attack Costs

Terrorist intent to cause economic harm

Current security and preparedness measures

Vulnerable target

Attack costs

group might plan against what kind of target reveals much about how high the attack costs will reach.

A group will base these decisions on whether its primary focus is the more traditional one of delivering a violent message or the more recent trend of imposing immediate and large-scale damage. Truly hobbling a large, stable economy is likely to be beyond the means of most terrorist groups.14 However, a variety of potential terrorist operations could produce sufficiently high costs to be of serious concern. High-end “macroterrorism” scenarios—attacks that produce sizable numbers of casualties and damage or destroy large amounts of property, such as the nuclear scenarios discussed previously—are the most obvious example of how a terrorist group could produce significant economic costs.

Beyond simply attempting to “scale up” their terrorist activities, another strategy for a group to use to maximize attack costs is to stage attacks with cascading effects that magnify the immediate damage and extend it over time. Examples of attack strategies capable of producing such cascading damage include

- targeting infrastructures on which a variety of interdependent economic activities rely—such as power grids15 or transportation networks (Haimes, 2005; Bae, Blain, and Bassok, 2005)
- using infrastructure networks as conduits to spread the effects of an attack itself. Agricultural terrorism is a commonly cited example (Chalk, 2004)
- staging contamination attacks on the food (Cremin, 2001) or water distribution systems.

14 Although large scale nuclear war could, for example, destroy a national economy (see, e.g., Sastry, Romm, and Tsipis, 1987), RAND analysis during the Cold War suggested that the economy could recover more rapidly than might be expected even after some nuclear exchange scenarios (Kennedy and Lewis, 1981). A recent analysis of how the broad-based conventional bombing of areas of Vietnam during the Vietnam War may have affected economic performance found no lasting economic impacts associated with even the high-density bombing involved in a major military conflict (Miguel and Roland, 2005).

15 For example, Chang, McDaniels, and Reed (2005); Lave et al. (2005); Rose, Oladosu, and Liao (2005); ICIS (2005); and Amin and Gellings (2005).
In contrast with macroscale attacks in which the damage is immediate, these scenarios focus on economic effects caused by broad *disruption* rather than on large-scale *destruction*. How attractive terrorists will find this type of approach will depend on how strongly they value economic effects in relation to other types of outcomes. Most macroscale attacks would produce their economic costs not just through disruption, but by inflicting major physical damage and numerous human casualties as well. A terrorist group may view this type of attack as more desirable because the attack results in what the group considers to be multiple benefits. Only a group that will be satisfied with few or no casualties will choose an attack that works primarily through disruption.16

**The Second Main Driver of Economic Costs: Perceptions That the Risk of Terrorism Is High**

The goal of generating fear lies at the heart of terrorism. Sustained fear can breed a pressure that may eventually lead decisionmakers to acquiesce to a terrorist group’s demands or take other actions that serve its interests. Economic targeting is no exception to this rule: In the aftermath of an attack, perceptions that the risk of additional terrorism is high and that the overall environment is insecure can cause governments, firms, and individuals to change their behavior, producing economic consequences.

It is useful to think about the perception of risk as being a function of two factors:17

- *Perceptions of the terrorist threat:* Organizations and individuals build expectations about the nature of future attacks. They develop beliefs about the probable type, frequency, and location of attacks—whether attacks are likely, what scale and type of damages will result, how frequently they will occur, where they are likely to take place, and what are likely targets. The perceived threat may or may not reflect the actual level of terrorist threat.18

- *Perceptions of the effectiveness of security and preparedness measures:* Effective measures can cause attacks to fail, limit an attack’s effects, and reduce the chance that the same terrorist group will wage repeat attacks. Individuals and organizations develop beliefs about how effective current security and preparedness measures are.19

---

16 Such groups might gravitate toward attack vectors that terrorists do not generally consider attractive. For example, despite their limited visibility and shock value, cyberactivities, such as hacking and releasing viruses, offer the possibility of inflicting costs at comparatively low risk, which increases their appeal if the goal is purely economic targeting.

17 See Moore and Shepherd (2006) for an example of economic measurement of the effects of fear or Jonathan Jackson (2006) for a discussion of fear of crime more broadly defined.

18 “Actual risks are extremely hard to assess. Not only are there few unbiased data available, but there is also much evidence that people, and by extension policy makers, are poor judges of objective levels of risks. Especially when strong emotions such as fear are involved, people tend to focus on worst case scenarios rather than on the probability of the outcome occurring. As a result, agents overestimate minor risks and neglect significant risks” (Brück, 2004, p. 106). See also Brück (2005).

19 Perceptions of the effectiveness of security measures may or may not be directly correlated with such inputs as resources spent on security initiatives.
In this simplified construct, risk is perceived if the level of effectiveness of security measures is considered insufficient to negate the perceived terrorist threat. The *match* between the perception of threat and of security is what is important: Whatever the perceived level of threat, if people believe that the security measures in place are enough to address it and that the two are appropriately balanced, then they judge the situation generally secure, and their perception of risk will be minimized or eliminated.\(^{20}\) If they see the two as not well balanced, a perception of insecurity will result.\(^{21}\)

A perception of risk can produce behavioral changes, leading to economic costs. Similarly, fear can increase the demand for security and preparedness expenditures, compelling government and businesses to take measures to protect against the threat. These security and preparedness measures can be costly, contributing to the overall economic cost of terrorism. In both senses, then, a terrorist group has good reason to try to make as broad a population as possible feel insecure: A heightened perception of risk drives costs higher. Figure 4.2 illustrates this balance and the costs that a perceived risk of terrorism can produce.\(^{22}\)

The most direct and obvious way in which a terrorist group can manipulate this balance in its favor is successfully staging an attack: Then an event that someone may have previously deemed unlikely becomes a much higher probability in the public mind. In reality, this may

---

\(^{20}\) Fielding (2003) discusses the measurement of subjective levels of insecurity in populations.

\(^{21}\) Government, businesses, and individuals will measure the terrorist threat and the effectiveness of security and preparedness measures differently. They will also differ on what constitutes an “appropriate balance” between them and how to respond when they deem them out of balance. A comparatively risk-tolerant actor might respond only when the “excess threat” reaches a certain threshold and then might react only slightly as the threat increases beyond that; a comparatively risk-averse actor is likely to respond immediately to an excess threat and strongly to any further increase.

\(^{22}\) Note that the effects of this balance can tip the other way as well—if the perceived level (and effectiveness) of security measures is viewed as excessive given the perceived threat, this could produce demand for reductions and potentially other changes in economic behavior.
or may not be the case, although, in the aftermath of an attack, a terrorist group may take actions to reinforce the idea that future attacks should be viewed as more likely.\textsuperscript{23} If the means of attack is novel or the location unprecedented, fear tends to increase even more. For example, discussions generated after Aum Shinrikyo’s attack on the Tokyo subway with chemical weapons or after Chechen terrorists attacked the school at Beslan are examples of how specific types of attacks can significantly shape public views of threats.

As for security measures, people tend to view their effectiveness in a binary fashion: Either they succeed in preventing attacks or they do not. This is not necessarily the only or most appropriate way to view the performance of security measures. But when a successful terrorist attack occurs, people who adopt this view will likely decide that, by definition, whatever security measures in place at the time have failed.\textsuperscript{24} This affects the other side of this balance, also leading to a perceived increase in terrorism risk.

Government, businesses, and individuals often alter their behavior and prioritize security and preparedness on the basis of perceived levels of threat and imperfect information on the effectiveness of security measures, rather than on objective measures. Consequently, reactions to the threat of terrorism—e.g., demand for a greater or lesser level of security—may not be economically optimal in relation to actual risk and effectiveness.\textsuperscript{25,26} As a result, both types of costs can accrue even in the absence of a terrorist attack.\textsuperscript{27}

**Linking the Perception of Risk to Economic Costs:**
**Two Ways in Which Fear Can Become Costly**

The 9/11 attacks and PIRA’s terrorist campaign provide examples of how the perception of risk can drive the economic costs of terrorism. Specifically, a belief that the risk of terrorism is high can lead government, businesses, and individuals to (1) change their behavior in response to the risk, and (2) increase their demand for security and preparedness measures.

\textsuperscript{23} Sarte (2004) describes a terrorist attack as having two features: “(i) it destroys capital . . . [and] (ii) it causes a permanent update in the probability of a future attack . . . that changes the perceived return to investment. In other words, one never again believes that one lives in a safe world, and this feature essentially acts as a tax on capital.” We agree that a first terrorist attack in a given area would cause this reaction. But if people were exposed repeatedly to terrorism over time, they would not necessarily feel that, with each new attack, the probability of yet another attack grew greater.

\textsuperscript{24} Terrorist organizations have long sought to demonstrate the failures of targeted governments to protect their populations.

\textsuperscript{25} See Brück (2004, pp. 112–113) for a more extensive discussion of preferences with respect to security.

\textsuperscript{26} Because of the costs associated with collecting information, all decisionmakers invariably make decisions based in part or in total on imperfect information and perceptions of reality. Because information on the terrorist threat is costly to collect (and, when collected, frequently kept secret) and because objective information on the effectiveness of security measures may be kept secret to deny adversaries data that could aid their efforts, judgments in this area will likely always depend on less information than would be required to produce economically efficient outcomes.

\textsuperscript{27} Brück (2004, p. 105) suggests that the economic costs of responding to insecurity may dwarf the costs of the security threats themselves.
Both of these outcomes can be expensive; each contributes to the total cost of economic targeting. Given a sufficient level of perceived risk, worries alone about the possible economic damage of terrorism may actually be enough to cause that impact to occur.28

**Changes in Behavior in Response to the Risk of Terrorism**

Businesses and individuals may take a range of actions in response to their expectations about the future security situation. All can drive the total cost of economic targeting higher.

**How Firms Can Change.** Businesses factor in the costs of operating in a riskier environment when considering new ventures and investments.29 An increased perception of risk can lead them to substitute less risky options to limit their exposure or address the potential consequences of terrorist activity.

On the one hand, such substitution behavior can be an advantageous response mechanism in the wake of a terrorist attack. For example, businesses that a terrorist incident affects and that can substitute other goods, services, or transportation modes for those unavailable or affected by the incident can reduce the actual costs caused by an attack (Hall, 2004). This type of flexibility could be one way to blunt an attack’s economic effects. If individuals have many sources of key products, the economy can recover if some sources are destroyed. If individuals who use a given network have many choices of interconnections and routes, operations can withstand damage to any single route. In studies of targeting during the Cold War, researchers concluded that, because major economies can compensate for damage in this way, if the goal were to produce a sustained economic disruption, it was better to target entire single industries rather than elements of all industries throughout an economy (e.g., Kennedy and Lewis, 1981).30

But substitution behavior can also increase the cost of terrorist activity. A perception of terrorist risk in one area may lead firms to locate in places and invest in ways that they might not otherwise have done.31 The companies that opted not to locate in London in the early 1990s as a result of the PIRA bombings are a vivid example of the former. Reports of Middle Eastern investors pulling investments out of the United States after 9/11 illustrate the latter.

Such cases are not isolated examples. Animal rights terrorist groups in the UK have adopted a similar strategy to target not a country, but individual companies. In addition to directly attacking firms that conduct animal testing, the groups have also threatened investors,

---

28 “Economists point out that expectations can be self-fulfilling. If businesses believe that consumers will respond to an increased uncertainty by cutting back on spending, it seems likely that they will reduce capital investment” (Bird, 2002, p. 107).

29 An extensive literature demonstrates how businesses often base location, or relocation, decisions on local crime rates.

30 A terrorist group that wants to maximize economic costs must minimize opportunities for its adversary to use this kind of substitution to limit damages. Advantageous targets from this perspective include critical industries in which an individual attack can damage a substantial part of available capacity; key chokepoints in communication nodes or infrastructures (e.g., key ports; see Gordon et al., 2005; and Park et al., 2006); or industries in which substitutes do not exist.

31 For example, country risk analysis focused on assisting firms making investment decisions in other nations (Meldrum, 2000).
customers, insurers, and banks in an effort to damage the companies’ business.\textsuperscript{32} The threats attempt to cause those organizations to substitute other firms or investment opportunities for the targeted companies, thereby advancing the terrorists’ goals.

These strategies can be very “high leverage” for a terrorist group. Companies at a distance from the real target of the terrorism have little incentive to resist terrorist pressure: They can invest their resources or take their business elsewhere.\textsuperscript{33} The more attractive the possible substitutes, the smaller the perceived risk needs to be to produce the response the terrorist group desires.\textsuperscript{34} This increases the chances that even small groups can generate significant economic effects.

Broader studies of terrorism’s economic effects have documented such substitution effects in other measures of economic activity, such as trade and FDI. According to one study, “a doubling in the number of terrorist incidents is associated with a decrease in bilateral trade by about 4%” (Nitsch and Schumacher, 2004). Similarly, levels of violence affect FDI, with the risk environment shaping how much is invested and where (Rogers, 2000). A standard deviation increase in the risk of terrorism in a country “induces a fall in the net FDI position of about 5 percent of GDP” (Abadie and Gardeazabal, 2005). In Spain and Greece during periods when terrorist groups were very active, terrorism reduced annual net FDI by an average of 13.5 percent and 11.9 percent, respectively (Enders and Sandler, 1996).

Businesses may also make other changes in their behavior, including

- \textit{the way they allocate resources}. Firms may take a variety of steps to hedge a perceived risk of terrorism. They may increase spending on risk management and insurance, increase their inventories (OECD, 2003a; Czinkota and Knight, 2005), or change their investment mix to safer or less vulnerable financial instruments.\textsuperscript{35,36,37} For example, Fielding’s analysis of Israeli investment behavior during the Palestinian intifada showed a significant depression of investment in nonresidential construction and in machinery and equipment investment, limiting the potential for future growth (Fielding, 2003b).
- \textit{what and how much they produce}. Firms continuously make assumptions about the likely demand for their products from other sectors and consumers. Perceived insecurity and

\textsuperscript{32} See, for example, BBC News (2001a, 2001b, 2002b); and Cox and Vadon (2004).

\textsuperscript{33} Attacks of this kind could even be viewed as creating a “fiduciary responsibility to capitulate.” Unless a firm can articulate a longer-term benefit to resisting terrorist pressure, accepting increased short-term costs and risks to its own financial interests by standing up to the terrorist’s demands may not appear to be in the interest of the firm’s shareholders.

\textsuperscript{34} Recent developments may actually have made it harder for a terrorist group to utilize this strategy. Because terrorism is now a global phenomenon, fewer countries are readily identifiable as low-risk substitutes for countries subject to attack.

\textsuperscript{35} “Several empirical studies, based on different techniques, approaches, and data, have found an inverse relationship between different measures of political instability and violence on the one hand, and growth or investment on the other” (Gupta et al., 2004, p. 405, and sources cited therein).

\textsuperscript{36} “Uncertainty negatively affects the capital accumulation process and the existence of instruments to share and limit risk—which help reduce uncertainty—are often associated with increased investment” (OECD, 2002, p. 125).

\textsuperscript{37} Data from the European Central Bank indicated a shift in investments after the 9/11 attacks to more liquid and safer short-term asset classes, a trend that persisted until early 2002 (European Central Bank, 2001, p. 5; European Central Bank, 2002, p. 7).
perceptions of how others will respond to that insecurity shape those assumptions. If a business assumes that the threat environment will decrease the demand for its goods (or increase it, in the case of security products), it may proactively change production in anticipation of expected market changes (Czinkota and Knight, 2005). Production changes can, in turn, result in shifts in hiring and other activities (see Padgham and Rossiter, 2005).

**How Individuals Can Change.** After a terrorist attack, when comparable choices are available, individuals tend to buy at, locate, invest in, and travel to places where they perceive the risk of terrorism to be lower. When a region, nation, or firm targeted by the terrorist group depends economically on these individuals, this substitution behavior can lead to increased losses. This, in turn, drives the overall cost of economic targeting higher.

As we saw in both the 9/11 and PIRA examples, tourism is a prime case, in which areas hit by terrorism are clearly hurt as individuals pass them over in favor of locales they perceive as safer (see Enders, Sandler, and Parise, 1992; Drakos and Kutan, 2003; Ito and Lee, 2005, p. 75; Fleischer and Buccola, 2002; Enz and Canina, 2002; and Stafford, Yu, and Armoo, 2002):

> Individuals planning their holidays are less likely to choose a destination with a higher threat of terrorist attacks. Host countries providing tourism services, which can be easily substituted, are, therefore, negatively affected by terrorist attacks to a substantial extent. (Frey, 2004)

Even a small increase in the perception of risk at a certain location can lead people to substitute other possible destinations. Examples and analyses of this behavior are plentiful:

- Between 1974 and 1988, international terrorism diverted tourists from specific countries (Greece, Italy, and Austria) and continental Europe overall, at a cost estimated in the tens of billions of dollars (Enders, Sandler, and Parise 1992).  
- There were significant effects on demand for hotel rooms as a result of the level of violence in Israel, with differences in the effect on local residents versus international travelers (Fleischer and Buccola, 2002).

---

38 Whether these individual industry impacts produce a net effect on the national economy depends on whether people substitute other economic activities (e.g., using other modes of transportation instead of airline travel, spending money on other goods or services that they would have otherwise spent on tourism) and any differences between how the effects of these alternative expenditures cascade through employment and production in other sectors and what would have happened had the attack not taken place.

39 Note that this analysis does not include terrorism not defined as international terrorism because of the nature of the data sources used.

40 Drakos and Kutan (2003) found similar effects.
Following the July 7, 2005, attacks on London’s Underground, rates of travel to London fell (Jordan, 2005).

After the 2002 attacks in Bali, Indonesia, tourist arrivals reported dropped 60 percent in the month after the attacks and cost the Indonesian economy approximately $1 billion (Australian Department of Foreign Affairs and Trade, 2004, p. 6).

In all of these cases, the terrorist group involved used a direct attack on a particular target to influence the behavior of individuals only remotely linked to that target. These individuals altered their behavior because they felt they were at greater risk of injury should they travel to the affected area. That decision resulted in economic losses for businesses and government in the area.41

In addition to opting for an alternative to a targeted area or business, individuals may change other types of behaviors, including

- **how and how much they invest.** A perception of heightened threat can lead investors to buy or sell securities based on their beliefs about the threat environment’s impact on those firms. This can include broad price depressions in stock markets (of varying duration) (see Eldor and Melnick, 2004; and Chen and Siems, 2004), as well as penalization of firms thought to be most at risk from terrorism (e.g., located in terrorism-prone areas, very involved in international trade, potential targets such as airlines) (see Hergert, 2004; Kim and Gu, 2004; Abadie and Gardeazabal, 2003; and Drakos, 2004). Conversely, individuals might gravitate to firms whose businesses are connected with combating terrorism (Berrebi, 2004, pp. 150–180). People may shift their investments away from productive assets toward less productive ones—for example, buying gold rather than making bank deposits or stock investments (Bird, 2002; Fielding, 2003b).42,43,44

- **how they spend and consume.** There is little consensus on how terrorist violence affects consumer behavior. Some argue that violence leads individuals to spend more instead of save, because the terrorist threat devalues putting money away for the future. In Israel, for example, terrorist violence may have been responsible for depressing savings rates by

---

41 From the terrorist’s perspective, these substitution effects may be more difficult to use against large countries and economies than small ones. With more area, more cities, and a more diverse economy, a large country may have more potential internal options for substitution. In the United States, for example, a terrorist attack in one city may compel visitors to go to another U.S. city but not outside the country. The nation’s size and breadth are a strength. This sort of internal displacement would be less likely in smaller countries, where an attack in one location would likely increase the perception of risk for the nation as a whole.

42 “[M]ovement of funds away from productive assets (bank deposits, capital) to non-productive assets (gold)” (Gupta et al., 2004, p. 405, and sources cited therein).

43 A study of Italian college students suggested that, after 9/11, students adopted more conservative risk behavior: “a more conservative weighting of low probabilities of gain, as well as [an] overemphasis on the probability of losing” (Sacco, Galletto, and Blanzieri, 2003, p. 1125).

44 After the 9/11 attacks, McKibbin and Stoeckel (2001) simulated the effects such reappraisals in equity risk premium over a five-year time frame could have on nations’ GDP performance. Depression of GDP ranged from approximately –0.6 to –1.0 percent, with gradually decaying effects that persisted even beyond the point at which investors’ risk perceptions returned to preattack levels. See also Australian Department of Foreign Affairs and Trade (2004).
almost half (Fielding, 2003a). Conversely, others suggest that violent instability deters consumption among some categories of consumers (Becker and Rubinstein, 2004; Eckstein and Tsiddon, 2004; Cukierman, 2004). This lack of consensus reveals that considerable uncertainty remains in anticipating the likely economic impacts from changes in consumer behavior (Hand, Paez, and Sprigg, 2005, pp. 24–25; see, for example, discussion in Frey, Luechinger, and Stutzer, 2004).45

- *how they behave at work.* Individuals may change their work activities in response to a perception of increased risk. The same factors that could lead to changes in consumption as people discount the future compared with the present could change incentives for participation in the labor market. Some changes in behavior link directly to the effects of an attack: for example, increases in worker absenteeism resulting from traumatic strain related to the 9/11 attacks (Byron and Peterson, 2002).

**Increases in Demand for Security and Preparedness Measures**

A successful terrorist attack increases the perception of danger both by causing a perceived increase in the threat level and by calling the effectiveness of current security measures into question. When government, businesses, or individuals perceive a residual risk of terrorism and the potential costs that risk implies, the natural desire is to boost security and become better prepared. This desire can lead to large outlays, which produce their own economic costs. Any one of the three may devote their own resources to security, or demand that others do so. Businesses, for example, might spend on security for three reasons:

- an internal desire to hedge risk46
- “market” demand from employees and customers for particular protections (see also Alexander, 2004, p. 114)

---

45 “Despite what economists know about risk and uncertainty, its meaning for modeling responses to large shocks or terrorist attacks is, in a word, uncertain. From the consumer point of view (and the same argument could be made for the producer side), a likely scenario is that a terrorist attack increases the perceived probability of future economic hardship, and consumers respond by reducing current consumption. But consumer response to a terrorist attack depends on agents’ perceptions of how event probabilities change, the individual level of risk aversion, and how expectations are formed; thus, as recent history suggests, a large shock will not necessarily lead to a large economic impact” (Hand, Paez, and Sprigg, 2005).

46 The assumptions that businesses make about how individuals, other firms, and government will behave in the event of a terrorist attack could also have the opposite effect. For example, the amount of compensation that firms or individuals expect to receive after a terrorist attack will presumably affect the economic decisions they make in response to the terrorism threat. If businesses or individuals can expect compensation for losses, tax deductions for property damaged in attacks, or tax incentives to rebuild, they are likely to be more willing to locate in areas at higher risk for terrorism and make investments that would not seem attractive otherwise. The cost and availability of terrorism insurance and expectations about liability for losses incurred by other firms and individuals may also factor into decisions made in the face of terrorism risk.
A government may increase spending on security and preparedness in response to the demands of a citizenry that perceives the level of risk to be high.\textsuperscript{47}

In this sense, terrorists have incentives to find ways to create doubt about the effectiveness of security measures. Demonstrating that a system currently thought to be secure has vulnerabilities might have a greater economic impact than would penetrating a system already thought to be ineffective, because the former may have a greater influence on the perceived level of terrorist risk. Similarly, hoaxes and false alarms can also be used to heighten the perception of ongoing risk, driving the overall cost of economic targeting higher. PIRA, for example, coupled actual bombs with hoax bomb threats. The real attacks meant that all threats had to be treated as genuine until proven otherwise. One former law enforcement officer referred to this as “ten penny terrorism,” because all it cost was change for the public phone to make the call (personal interview, May 2005). A group that can craft attacks more likely to be followed by hoaxes and false alarms has the potential to multiply economic damages considerably (Rogers, 2000).

\textbf{Summary}

Figure 4.3 brings together the three categories of costs associated with economic targeting and illustrates their interrelationships. Attack costs are driven by the combination of a terrorist group’s intent to cause large-scale damage and whether or not current security and preparedness measures leave vulnerabilities in a potential target that the group can exploit to produce significant economic costs. Without a successful attack, there will be no attack costs.

In contrast, costs in the other two categories can accrue whether or not an attack actually occurs. If government, businesses, or individuals perceive a risk of attack (resulting from a perceived mismatch between the threat level and current security and preparedness efforts), the outcome may be an increase in demand for security and preparedness expenditures, costs produced by behavioral changes, or both.\textsuperscript{48}

In shaping the overall cost of economically targeted terrorism, security and preparedness investments are key, for, as additional investments are made, they feed back to affect both potential attack costs (assuming that they are effective) and the perception of the terrorism risk (assuming that they are perceived to be effective).

Although our simplified framework (Figure 4.3) does not capture the full complexity of the interplay between terrorism and national economies, it is useful for thinking through defensive options to counter this threat.

\textsuperscript{47} Discussing the growth of “the security industry,” Stevens cites general increases in demand by individuals, businesses, and government for security products and services (Stevens, 2004).

\textsuperscript{48} Note that these costs are not necessarily simply additive, as they may manifest differently over time and have different consequences on different economic actors (e.g., individuals versus firms versus government).
Figure 4.3
Conceptual Framework for Examining Economically Targeted Terrorism

First cost driver

Terrorist intent to cause economic harm

Perceived threat level

Imbalance causes perceived terrorism risk

Current security and preparedness measures

Perceived security and preparedness effectiveness

Vulnerable target

Demands for more security and preparedness

Security and preparedness costs

Changes in economic behavior

Behavioral change costs

Feedback to level of perceived security and preparedness effectiveness

Perceived threat level produces Balanced?

Attack costs
As the examples of al Qaeda’s attacks on 9/11 and PIRA’s campaign of terrorism in Great Britain and Northern Ireland show, economic targeting can be a dangerous and costly terrorist strategy—whether alone or as part of a larger plan. Clear policies addressing the damages economic targeting can cause and, ideally, limiting terrorist groups’ ability to successfully harm an economy are an important part of a comprehensive defensive effort against terrorism.

Preparing the nation for economically targeted terrorism presents considerable challenges, however. Implementing a defensive strategy to protect the nation requires action not just by government, but by individuals and firms as well. Just as each can be a victim of economic targeting, each has a role in defending against it. In some cases, actions that an independent party may take to protect itself will also serve to protect the nation more broadly. But often, individual and national interests do not coincide. For a response to economic targeting to succeed at the national level, government, businesses, and individuals at all levels within an economy must have clear incentives and guidance for responding to this threat in ways that work together to serve their multiple interests.

Two Policy Levers to Guide National Responses to Economic Targeting

A terrorist group’s ambition to stage a large-scale, high-cost attack and perceptions that the risk of terrorist attack is high both drive the costs of economic targeting. These two drivers point, in turn, to two possible policy levers that might be used to shape public, private, and citizen responses to this threat:

- The first and most straightforward is to reduce the potential attack costs of future events. One approach is to lower the probability of a successful attack; another is to limit the consequences of attacks that are successfully carried out.¹
- The second is to take actions that shift the perceived level of terrorist risk, thereby reducing the potential for security and preparedness and behavioral change costs.

¹ The relationship between probability and severity may be complex. Indeed, by implementing a policy to reduce the severity of a potential event, the government may, at the same time, reduce the probability that the event will ever happen: The policy designed to reduce the severity makes the potential target less attractive.
We present four options that illustrate the range of tactics that might be used to apply these two levers: (1) security and preparedness measures, (2) robustness and resilience measures, (3) insurance and compensation, and (4) public information and risk communication.

**Security and Preparedness Measures**
Investments in security and preparedness measures are often the highest-profile response to terrorism, both economic and otherwise. They have the potential to shape the costs of terrorist attack both directly and indirectly by

- reducing the probability of economic attacks succeeding (and, accordingly, attack costs being incurred) in general or at sites of particular concern
- limiting behavioral responses by improving the match between the security level and preparedness and the perceived threat level.

Because measures in this category can directly reduce the immediate costs of attacks, decisionmakers frequently give them priority. Government (at the federal, state, or local level) is often best positioned to secure economically important targets. But in the case of privately owned sites, it may be better for the private sector to take action. Individuals can contribute by preparing themselves for terrorist events (Farmer, 2004, and Brück, 2004).

But because these measures come with a price tag, caution is needed so that the resources devoted to them do not end up generating the very costs a terrorist group aims to impose. From a purely economic viewpoint, the decision to implement security and preparedness measures should be driven by whether the benefits of added investment outweigh the costs of doing so. Additional resources should be allocated until the marginal benefits (i.e., reductions in expected attack costs or costs resulting from behavioral changes) no longer exceed the marginal costs. This guideline recognizes the reality that implementing this class of measures can have both the intended effect—namely, to decrease the costs of economic targeting—and exactly the opposite one.3

Putting this principle into practice is not always straightforward, however. The links between attack, security, and preparedness, and behavioral change costs and the difficulty of anticipating terrorists’ future behavior make estimating the potential costs of terrorism (and, therefore, the benefits of security and preparedness measures) problematic. That, in turn, makes it hard to estimate optimal levels of protective measures.

Furthermore, the economically desirable level of protection may differ from various perspectives—for example, the federal government’s compared with that of an individual city. Although displacing economic activity from one part of the country to another after an

---

2 Although the full range of approaches to the problem of terrorism—including, for example, intelligence and law enforcement action—helps reduce the potential economic damages from attack, addressing all such strategies is beyond the scope of this document. These broader counterterrorism activities clearly contribute to the effectiveness of the more “purely economic” approaches we describe here and should be examined and assessed in tandem with them.

3 This balancing act can be seen in a recent study that used a comprehensive input-output model to examine a range of costs resulting from security and preparedness measures triggered by changes in the DHS threat level (Haimes, 2005).
Defending Against Economically Targeted Terrorism

Attack might not have a net effect on the nation overall, it could be very important locally. Similarly, the actions that individuals take to protect themselves may or may not translate into increased protection for the nation. For example, security improvements around a power-generating plant will shield many companies from losses—not just the power company—if they prevent an attack at the plant. But in others, protective actions that shield an individual firm from attack shift the risk to other firms. Although this may be privately beneficial, it does not change the total terrorism risk to the nation. These differences further complicate thinking about appropriate investment levels. Moreover, they could produce added pressure to do more to protect the country—risking overinvestment in security and generating the very economic costs the policy was intended to prevent.5

Robustness and Resilience Measures

Another category of preparatory measures can contribute not to preventing an attack altogether, but limiting the damage a successful attack can inflict. An economy’s robustness (as well as particular networks within it) is its ability to limit an attack’s damage by failing in ways that will contain the attack’s effects to the fullest extent possible.6 Measures that increase robustness include:

- Emergency response and rapid damage containment capabilities7
- Technologies that provide “circuit breakers” to contain failures within systems
- Maintenance of redundant elements in systems so that when individual pieces fail in an attack, broader economic damage is less likely.8

Robustness can be built through a variety of mechanisms. The design of infrastructure networks can be changed to reduce their vulnerability to large-scale failures, for example (Petroski, 2004).

Resilience has been defined as an economy’s ability to reduce the damages that occur from a severe shock by rapidly adjusting to and addressing its consequences. Two types of resilience have been identified in economic systems (Rose, 2004):

- Inherent resilience is the flexibility built into markets’ and businesses’ everyday operations that makes it possible to adjust to changes in the environment or damaging events.

---

4 Viewed from the perspective of the market, such displacement might be a rational, and perhaps even efficient, response to the change in threat but might still result in other undesirable costs or changes in the nature of the national economy.

5 See, for example, Lakdawalla and Zanjani (2005) for discussion.

6 In some contexts, measures that reduce the probability of failures for some or all networks or economic systems would be alternatively labeled as mitigation.

7 For example, the measures put in place in the World Trade Center after the structure was bombed in 1993—including backup lighting and luminous paint in stairwells to help speed evacuation (Carey, 1997)—were credited with greatly reducing the number of lives lost in the 9/11 attack (Kugler, 2001).

8 Branscomb (2004) and Emily Smith (2002) discuss a variety of such measures.
Economically Targeted Terrorism

Examples include substituting other inputs for those curtailed by an external shock or letting markets reallocate resources in response to price signals.

- **Adaptive resilience** is the ability to change how things are done during a crisis situation (through ingenuity or extra effort) to provide flexibility beyond what everyday operations provide. Examples include increasing possibilities for substituting input in individual business operations or providing information that will match suppliers without customers to customers without suppliers.9

Additional resilience can be gained if businesses or individuals can shift their activities to a time after the consequences of the damaging event have passed. A good example would be a firm’s ability to “make up” the production disrupted by an attack after key infrastructures come back online, thereby reducing the total costs of the interruption (Rose, 2004, 2005).

Disruptions in supply or demand are a frequent source of economic damages in the wake of an extreme event. Either goods or services cannot be produced or delivered where they are needed, or customers that, under normal circumstances, would have purchased goods cannot or will not do so as a result of the changed risk environment. An emphasis on maintaining redundancies and strengthening systems’ ability to tolerate extreme events can cushion the economic costs of disruptions in supply or demand (Branscomb, 2004; Emily Smith, 2002).10

Strategies to protect specifically against supply disruptions include

- maintaining slack capacity and backup facilities
- preplanning how firms will allocate products to customers in the event of scarcity to avoid damaging inefficiencies
- building more flexibility into production systems so they can be scaled up and down rapidly
- ensuring access to multiple sources that can provide needed goods and services (Sheffi, 2001; Batterman and Fullerton, 2002).

The government could implement such strategies on its own. Actions taken by the Federal Reserve after 9/11 to ensure the availability of sufficient liquidity provided such a “supply cushion” for the financial system.11 The Strategic Petroleum Reserve to cushion disruptions in the energy supply is another example. However, in most cases, these measures must be implemented by the private sector.

Measures to reduce the chance that an event will result in disruptions in demand include

---

9 See, for example, discussion of building adaptive resilience in maritime supply chains in Barnes and Oloruntoba (2005).

10 See Willis and Ortiz (2004) for a discussion of these issues with respect to a specific infrastructure system.

11 Responses to 9/11 of the Federal Reserve and the payment system are discussed in Lacker (2004), Williamson (2004), and Lang (2001).
• using “psychological hardening” or “psychological preparedness”\textsuperscript{12} to reduce the effects of terrorism on individual and firm behavior
• exhorting consumers to continue spending, for example, as a way of reducing disruptions in demand for consumer goods
• increasing direct government spending to provide a stimulus
• providing mechanisms to cushion the effects of behavioral shifts on the economy more broadly, such as systems to help bring together buyers, whose sources of supply may be disrupted, and sellers, whose production capacity is functional, but who may lack customers.

Other measures can help address disruptions in both supply and demand; for example, government or sectoral inventories of critical intermediate goods or final products. In the event of a crisis, drawing on such an inventory can create a cushion on the supply side, while continued purchases that replenish it provide a stable buyer that cushions on the demand side.

Decisionmakers tend to think of resilience and robustness measures in the context of the catastrophic, shocklike events characteristic of episodic terrorism. But measures of this sort are similarly applicable—if in somewhat different ways—to an economy’s ability to continue functioning effectively in the less certain environment of ongoing, campaign terrorism (Omand, 2005). In an episodic event, robustness and resilience reduce the impact of the initial shock and subsequently dampen its impact as it moves through the economy. In a campaign, robustness may significantly lessen the impact of numerous small-scale events and resilience, if the flexibility it provides limits the impacts of such attacks, could make an important contribution to reducing the impact of the ongoing threat of attack on economic behavior.

But building robustness and resilience on a national scale can be difficult. Again, the frequent mismatch between public and private incentives comes into play. Private motivations frequently dissuade firms and individuals from investing in resilience and robustness measures that would have broader public benefits.\textsuperscript{13} Economic competition and profit incentives push toward lean (e.g., just-in-time) production systems, concentration of resources to produce scale economies, and coupling of infrastructures to leverage benefits from scale and interconnectedness (Branscomb, 2004).

The price of resilience and robustness, then, is the costs associated with the inefficiency of maintaining slack capacity and building stronger systems than most circumstances necessarily require. This defines a tradeoff for both public- and private-sector decisionmakers that ranges along a spectrum. At one end are expensive, highly resilient and robust systems capable of continuing to operate under the most demanding of circumstances. At the other are productively efficient but vulnerable systems that may operate effectively under most circumstances but fail readily under stress. The question is whether businesses will heed the market forces that inherently push toward efficiency but can create vulnerability or will opt to build robustness and resilience into infrastructure and other systems. To lead them to make choices that serve

\textsuperscript{12} These concepts are discussed in a range of recent policy documents relating to terrorism preparedness, summarized in Grimmett (2004), Butler (2003), Tucker (2003), and National Science and Technology Council (2000s).

\textsuperscript{13} See Orszag (2003) for a broader discussion of private incentives and homeland security.
the national interest, either mechanisms must be developed that can price the risks associated with system failure or intervention must come from outside—e.g., standards or mandates that require companies to take specific risk management actions (or disclose their absence).

**Insurance and Compensation**

After a terrorist attack occurs, opportunities to affect the nature and scale of its costs become more limited. A major terrorist attack will affect many individuals and firms. Extensive action will be needed simply to address its immediate consequences and the subsequent hazards it produces. It may be beyond citizens’ and businesses’ ability to deal with its consequences in an appropriately coordinated and effective manner. Behavioral changes may be inevitable simply because individuals and firms lack the resources to make any other choice. Direct action is one way to address this problem. The government’s cleanup activities after the 9/11 attacks are a good example.

As an alternative to direct action to address the aftermath of an attack, compensation and insurance provide ways for the costs suffered by government, firms, and individuals directly affected in an attack to be transferred to others within the economic system. These mechanisms can move costs both from “level to level” (e.g., from businesses to government) and among similar actors within the economy (e.g., from affected firms to insurers or others). The rationale for reallocating costs in this way is twofold: to provide the resources needed for affected businesses and individuals to recover more rapidly (or, depending on their scale, make it possible to recover at all) and to reduce any additional costs that might result from changes in behavior made in response to the initial costs. As such, compensation and insurance have two objectives: First, they seek to “short-circuit” the connection between a perceived increase in the risk of terrorism after an event and behavioral changes that might produce additional economic costs. Second, they prevent cascading damages that might occur if affected sectors or firms cannot recover. Table 5.1 summarizes the range of insurance and compensation mechanisms that have or could be used to design policy responses.

A purely economic rationale for deciding how much postevent compensation and risk transfer to provide would be based on committing resources until the marginal benefits (in subsequent costs reduced) no longer outweighed the marginal costs of doing so. But once again, in determining where that balance lies, there may be real differences from the national, state, and local viewpoints and factors that have little to do with the economy may influence

---

14 For compensation mechanisms, see Dixon and Reville (2005), Sommer (2003), OECD (2002, p. 118), and Holtz-Eakin (2005). For insurance mechanisms, see Chalk et al. (2005); Saxton (2002b); Torregrosa (2002); Rhee (2005); Gron and Sykes (2002); Smetters (2005); Lakdawalla and Zanjani (2005); Kunreuther and Michel-Kerjan (2004); Brown, Kroszner, and Jenn (2002); Levmore and Logue (2003); Torregrosa (2005); Brown et al. (2004); Holtz-Eakin (2005); and Barker (2005).

15 Mechanisms that enable risk transfer or management or provide compensation for losses could also be viewed as measures that increase the economy’s resilience by addressing potential capital shortages after an attack.

16 Compensation mechanisms may also relate to other societal goals not economic in nature. For example, one rationale for the government to compensate for costs suffered in a terrorist attack on the nation is that it is inherently more fair for the country as a whole to bear those costs rather than have them fall disproportionately on a subset of individuals (Dixon and Reville, 2005).
Table 5.1
Insurance and Compensation Mechanisms for Reallocating Costs from Terrorism

<table>
<thead>
<tr>
<th>Instrument</th>
<th>From</th>
<th>To</th>
<th>Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insurance</td>
<td>Individuals</td>
<td>Firms</td>
<td>Medical, life, worker’s compensation, and property insurance</td>
</tr>
<tr>
<td>Firms</td>
<td>Other firms</td>
<td></td>
<td>Terrorism coverage for property, business interruption, and similar disruptions and losses</td>
</tr>
<tr>
<td>Firms</td>
<td>Government</td>
<td></td>
<td>Public insurance, reinsurance, or insurance subsidy</td>
</tr>
<tr>
<td>Compensation</td>
<td>Individuals</td>
<td>Other individuals</td>
<td>Charitable contributions and other compensation through nongovernmental means</td>
</tr>
<tr>
<td>Individuals</td>
<td>Firms</td>
<td></td>
<td>Charitable contributions and other compensation through nongovernmental means</td>
</tr>
<tr>
<td>Individuals</td>
<td>Government</td>
<td></td>
<td>Public compensation or direct subsidy</td>
</tr>
<tr>
<td>Firms</td>
<td>Government</td>
<td></td>
<td>Public compensation, direct subsidy, loans or loan guarantees</td>
</tr>
</tbody>
</table>

NOTE: Here, we show the transfer of costs as the payments made after a terrorist event from one actor to another. In actuality, insurance mechanisms are risk sharing in which firms act as intermediaries for the transfer of cost from the affected entities to the larger number of participating entities (e.g., property insurance transferring costs from affected policy holders to the larger pool of all policy holders with the firm acting as intermediary) making the actual transfer from one set of individuals (or firms, in the case of business insurance) to others.

decisionmaking. Particularly after a high-impact terrorist attack, there may be a very strong desire to restore the nation and its economy to their condition before the attack—either by preventing economic harm or by fully repairing any damage that does transpire. If some parts of the nation are bearing the economic burdens of the attack disproportionately, there may be an ardent call to “make things right.” This demand is consistent with fundamental mores of fairness—e.g., single individuals, firms, areas, or regions should not suffer disproportionately from a strike on the nation as a whole.17 This could provide a rationale for offering more compensation or risk transfer than might appear economically optimal from a national perspective.

Public Information and Risk Communication
Efforts to communicate with the public about the terrorist threat and security and preparedness measures and to provide other relevant information have the potential to shape individuals’ and firms’ perceptions of the terrorism risk level and to guide their behaviors in response to those perceptions. Accurate information is the basis for good decisionmaking. If indeed an imbalance exists between the security and preparedness measures in place and

17 The idea of restoring the status quo ante before terrorism affected the economy fits most readily for episodic terrorism—discrete, often large-scale, instances of terrorist violence. It is more difficult to apply in the case of campaign terrorism, in which attacks are repeated and the threat is ongoing. There, the concept of the status quo ante becomes less meaningful and policies are more difficult to maintain consistently.
Insurance Responses to PIRA Terrorism and the 9/11 Attacks

Insurance mechanisms were prominent in response to both of the examples discussed previously in this report, PIRA’s terrorist campaign in Britain and Northern Ireland and the September 11, 2001, attacks in the United States.9

Pool Re: The Insurance Response to Irish Republican Terrorism. The UK’s response to PIRA’s large scale and costly attacks in the London financial districts was government requesting that insurers form a mutual reinsurance organization specifically for terrorism risks. Initially, the losses that PIRA attacks had routinely produced defined the risks that the pool covered: fire and explosion. After 9/11, the risks covered were broadened to cover threats such as unconventional weapons. The pool covers commercial property losses and business interruption, but not personal losses or workers’ compensation. The pool acts as a reinsurer for its members, with the government acting as reinsurer to the pool providing access to resources above the pool’s reserves from the UK treasury. Membership is not mandatory. The terms of the pool define the amount of terrorism risk retained by industry and by individual firms for each attack. In the event of payment, participants would reimburse the treasury over time.

The Terrorism Risk Insurance Act (TRIA): Terrorism Insurance After 9/11. TRIA establishes a requirement that insurers make certain types of coverage for terrorism risks available under the same terms used for other major loss events. TRIA provides federal reinsurance for insured losses above a threshold for instances of foreign acts of terrorism. Initially, the threshold was set for incidents producing damages of at least $5 million up to $100 billion. With the extension of TRIA, the minimum incident size was increased to $50 million in 2006 and $100 million in 2007. Acts deemed domestic terrorism are not covered under the act. There is no premium paid to the government for this reinsurance. Insurers must pay a significant deductible, based on the size of their commercial property and casualty business, before government payments would begin. Government outlays in response to a terrorist attack can be recouped after the fact through a surcharge in the years after.

Additional detail of the terms and characteristics of both Pool Re and TRIA are available in Michel-Kerjan and Pedell (2006), UNCTAD Secretariat (1995), Torregrosa (2002), and Chalk et al. (2005) on which these summaries are based.

the level of terrorist threat, a realistic perception of risk provides an incentive for individuals, businesses, or the government to make reasonable investments to restore the balance or to put pressure on others (through the political process or the market) to do so. Frequently, government is in the best position to provide information both on the threat and on the measures taken in response to it. By taking the initiative, it addresses a market failure that would otherwise leave private individuals and businesses without the data they need to make decisions (Farmer, 2004).

But efforts to disseminate public information must be implemented carefully. If the information provided does not, in fact, reflect actual levels of threat or preparedness, it has the potential to create unnecessary costs.18 Inordinate expenses can accrue not just when the public underestimates the threat environment, but also when its estimates of the threat are unrealis-

---

9 Additional detail of the terms and characteristics of both Pool Re and TRIA are available in Michel-Kerjan and Pedell (2006), UNCTAD Secretariat (1995), Torregrosa (2002), and Chalk et al. (2005) on which these summaries are based.

tically high. Inflating the terrorist danger in public discussion risks generating a demand for more and more security or producing additional behavioral change costs.

**Issues to Consider in Crafting a Defensive Plan**

When a terrorist group’s goal is to cost a targeted nation money and money must be spent to address the threat, crafting a strategy in which money is spent wisely is not just good stewardship, but an integral part of successfully carrying out the counterterrorism mission. This gives cost-benefit analyses a strategic urgency.\(^\text{19}\) Policymakers should consider a number of issues as they assess options for responding to economically targeted terrorism.\(^\text{20}\)

**How Do Measures Perform in a Varying and Uncertain Threat Environment?**

Policymakers should examine how response measures may perform in a variety of different threat environments. In this way, they can limit the chances that preparedness measures will generate unintended consequences if the threat changes. If risk information can be obtained (or estimated) at reasonable cost, this can do much to help put measures in place that achieve the greatest benefit at the least expense. Spending on preparedness measures for targets only at limited risk of attack creates economic costs now without necessarily producing the compensating benefit of reducing potential attack costs.\(^\text{21}\)

The distinction between episodic and campaign terrorism is useful here. Appropriate policy responses for terrorist events viewed as exceptional departures from a normal state of affairs might not be practical when events are repeated. For example, if economic attacks are rare, generous compensation policies for affected individuals or organizations may be easier to implement than if attacks are common. In the first case, policies result in the equivalent of discrete payments. But for repeated terrorist events, compensation may produce an unpredictable and continuing obligation that extends into the future. If a compensation policy is designed in anticipation of a threat environment that does not materialize, it may be inappropriate to meet the needs it was intended to address.

---

\(^{19}\) Laying out approaches for rigorously calculating the costs and benefits of specific response options was beyond the scope of this study. Chow et al. (2005); Shaver et al. (2004); Martonosi, Ortiz, and Willis (2006) discuss cost-benefit approaches to specific counterterrorism security and preparedness measures. For example, Martonosi, Ortiz, and Willis calculate the costs of screening 100 percent of incoming cargo containers at ports. They bring together assessments of equipment performance, capital costs, staffing, and other relevant variables to determine the relationship between the perceived cost of delays to cargo at the port (an indirect but potentially substantial cost beyond those that can be readily quantified) and the expected probability and consequences of a terrorist attack via containerized cargo at which 100-percent screening becomes viable. Zycher (2003) describes an effort to develop broader preliminary estimates of the costs and benefits of counterterrorism more generally. For a much more detailed discussion focused on homeland security policies, see Smith and Hallstrom (2004).

\(^{20}\) See Chapman and Leng (2004) for a discussion of this type of analysis of different approaches for a specific potential target type.

\(^{21}\) The issues associated with integrating risk data and uncertainty into decisionmaking and resource allocation are beyond the scope of this analysis. They are discussed in detail elsewhere in the literature. See Willis et al. (2005) and references therein.
Given the uncertainties in predicting risk, an alternative approach is to assess the benefits of preparatory measures in the absence of terrorism risks.\textsuperscript{22} Some measures are highly specific to a terrorist threat: If the attacks to which they are designed to respond do not occur, they will have no benefits.\textsuperscript{23} Their outcomes are highly sensitive to any changes in the threat environment or misjudgments about it. But other measures may produce broader benefits that will accrue even if a terrorist event never takes place. For example, many infrastructures suffer frequent outages from accidents, weather, or natural disasters. The benefits of making these infrastructures more robust and resilient will go well beyond reducing damage from terrorist incidents. Similarly, even security technologies relatively specific to economic targeting may reduce (or at least displace) other crime in areas where they are deployed.\textsuperscript{24} For example, in London, the security and surveillance measures put in place to address terrorism risks reportedly reduce the level of non–terrorism-related crime significantly (McMahon, 1995). If security measures were designed in a certain way, they could also boost efficiency in other areas—for instance, advanced information tracking and sharing systems that might shorten port or customs clearance times (OECD, 2003a; Australian Department of Foreign Affairs and Trade, 2004).\textsuperscript{25}

Depending on the assumptions made about a specific threat of economic targeting, that portion of a measure’s benefits not related to terrorism could represent a substantial fraction of its total expected benefit. Given uncertainty about threat levels and how they evolve, such benefits could be designed into systems as guaranteed payoffs for the investment.

**How Do Measures Perform Over Time?**

Assessments of the benefits of specific measures must be made in a dynamic context, with the understanding that terrorist groups are adaptive adversaries who will change their behavior in response to the incentives generated by preparedness actions (Brian A. Jackson, Baker, et al., 2005a, 2005b). Producing incentives for changes in terrorist behavior is one goal of counter-terrorism strategies—for example, those which seek to deter adversaries from specific types of activities. But, when measures are put in place to limit a terrorist group’s ability to target an economy, the group should be expected to seek out alternative strategies: It might alter its targets, tactics, operational modes, and areas of operation in ways that reconstitute its ability to do damage and advance its interests.

\textsuperscript{22} This approach has been labeled a “dual benefit” strategy to preparedness (Ruth David, quoted in Branscomb, 2004, p. 277).

\textsuperscript{23} However, their costs may be similarly sensitive to the threat environment. A terrorism-specific compensation program may produce benefits only after an attack occurs; in the absence of an attack, it may be essentially costless. As a result, although the benefits of a policy option may be highly sensitive to the realized threat environment, its overall cost-benefit ratio may be much less so.

\textsuperscript{24} For example, in London, the so-called “ring of steel”—a security and surveillance cordon constructed around the central financial district targeted by PIRA—reportedly reduced the level of non–terrorist-related crime in the area significantly (McMahon, 1995).

\textsuperscript{25} “Exact” benefits from averting or reducing the impact of a terrorist attack could be calculated only given data on the probability and consequences of specific attack modes at specific targets. Such exact measures are inaccessible at reasonable cost, and policy is, in fact, driven by estimates of their magnitude.
Cost-benefit analyses of specific strategies must consider how robust those strategies are to the adversary’s adaptive behaviors. Are there ways in which terrorists can circumvent or neutralize countermeasures designed to keep them from inflicting economic damages? And, if yes, are the current defensive strategies similarly adaptive?26

**How Do Measures Reconcile National and Local, or Public and Private Incentives for Preparedness?**

In many cases, the benefits of specific preparatory measures may be very different at the local level—i.e., from the perspective of individuals, firms, or even specific locations—than at the national level. To build a successful national strategy, policymakers must address the differences in incentives between national and local, public and private actors.27 For example, private actors may have incentives to protect themselves either too little or too much when viewed from the perspective of society overall (Farmer, 2004; Lakdawalla and Zanjani, 2005). There may also be interdependencies among the choices of different stakeholders, as when the security choices of one firm affect the choices of others, for example. Such factors can significantly shift the incentives for investing in security (Coughlin, Cohen, and Khan, 2002; Heal and Kunreuther, 2005; Kunreuther, and Heal, 2003). Although it is beyond the scope of this analysis to examine specific solutions to these issues, implementing defensive approaches may require additional mechanisms to align private and public incentives. These include security and preparedness guidelines, financial incentives (e.g., taxes or subsidies), regulation or mandates,28 or inspection processes (Heal and Kunreuther, 2005; Kunreuther and Heal, 2003; Farmer, 2004).

**How Do Measures Shape Behavior Within the Economy?**

Though strategies to address economically targeted terrorism are designed to shape terrorist behavior, they shape the behavior of governments, businesses, and individuals as well. Sometimes, such shaping has positive outcomes. Developing guidelines for preparedness to spur firms or individuals to take action is an explicit effort to get their behavior to better match the threat environment.

However, some measures do have the potential to shape behaviors in negative ways as well. Actions that individuals or firms are willing to take to prepare for a terrorist attack will be significantly influenced by assumptions about the types of ex post measures that may be available if it actually occurs—for instance, insurance payments or other compensation for attack costs. Readily available compensation, to take one example, could generate a moral hazard to firms and individuals taking precautions they might not otherwise take and, therefore, reduce the real net benefit of specific policy options (OECD, 2003b).

---

26 See, for example, Brian A. Jackson, Chalk, et al. (2007).

27 See Orszag (2003) for a broader discussion of private incentives and homeland security.

28 Such approaches might be required where the information on which guidance is based cannot be broadly shared outside the government to protect sources of intelligence data.
When considering economic targeting, decisionmakers face several key issues:

- A full accounting of the economic effects of terrorism requires bringing together not only the costs caused directly by one or more terrorist attacks and the behavioral changes generated by the fear of terrorism, but the security and preparedness expenditures made in response. If the terrorists’ goal is to cost the nation money, part of denying them success is not overspending in efforts to counter the threat they pose.
- The effect of terrorist violence on an economy is shaped by whether it is seen as a shock—an infrequent, potentially large-scale exogenous influence—or as an ongoing characteristic of the economic environment.
- In crafting a strategy to target a major national economy, a terrorist group has a variety of options. The desire to inflict economic damages produces pressure to scale up attack operations to generate large immediate costs, take advantage of networks and infrastructures to produce cascading effects, or manipulate substitution behaviors to maximize costs. The terrorist’s ability to pursue any of these pathways depends on having the knowledge and capability needed to do so.
- In defending against economically targeted terrorism, the central policy levers available are investments in security and preparedness measures and actions to shape the public perception of the level of terrorist risk. There are different ways of doing both, with their benefits shaped by how the terrorist and other threats evolve over time.

As we conclude, it is reasonable to step back and examine the threat of economic targeting in a larger context. Studies of Cold War-era nuclear targeting and models of the economic effects of nuclear exchanges suggest that it would be very difficult for a terrorist group of reasonable capabilities to have a broad impact on a major national economy. However, setting aside whether it would be possible for terrorists to pose a strategic threat\(^1\) to a nation’s economic viability, there is broader disagreement in the literature about just how important an influence economically targeted terrorism and the expenditures made to address it are. These viewpoints range from significant concern about how the indirect effects of a terrorist threat impose costs

---

\(^1\) That is, the ability of a terrorist attack to “bring a major economy to its knees.”

49
on the economy (Brück, 2005) to the assertion that expenditures for security are small enough relative to the size of national economies that they merit little concern (Hobijn, 2002).

The total magnitude of the costs of economic targeting and their influence on the economy remains an open question, varying considerably over the range of possible terrorist scenarios. The goal of this report is to mine the available literature to examine the elements that contribute to economic damages from terrorism to understand how both the terrorist and defender might seek to exploit them for their own ends. Building the integrated economic model needed to reach definitive conclusions about not only the costs of specific types of attacks and how they cascade through the economy, but also the costs of the security and preparedness measures put in place to counter them was beyond the scope of our work. Research is currently progressing toward an increasingly detailed and integrated understanding of how the economic effects of terrorism play out. This knowledge will offer a basis for detailed judgments about such questions.

What we can say now is that, if costs are one of the measures by which a terrorist group assesses its success, then the resources expended on defensive measures must be carefully managed. Failure to do so risks contributing to the terrorists’ goals rather than our own. And although arguments can be made that security expenditures may be small when compared with the national economies they are intended to protect, it is not necessarily the absolute level of expenditures that is important when considering their potentially negative effects. More critical is what those expenditures are crowding out: Resources spent on security, for example, cannot be devoted to productivity-enhancing activities like conducting research and development or acquiring new technologies (OECD, 2002, p. 118; Gupta et al., 2004, p. 406) that help address other risks that also claim the lives of the nation’s citizens. Or resources used in this way impose their own costs on the nation’s economic development and progress (e.g., Gold, 2004, p. 2). If the threat of terrorism is claiming a significant fraction of the “discretionary resources” that might otherwise be invested in ways that pay broader dividends over time, then the impact of those expenditures may be disproportional to the costs caused by the attacks themselves.


CBO—see U.S. Congressional Budget Office.


ICIS—see Institute for Civil Infrastructure Systems.


OECD—see Organisation for Economic Co-Operation and Development.


Park, Jiyong, Peter Gordon, James E. Moore, and Harry W. Richardson, “Simulating the State-by-State Effects of Terrorist Attacks on Three Major U.S. Ports: Applying NIEMO (the National Interstate Economic


http://purl.access.gpo.gov/GPO/LPS25535

http://purl.access.gpo.gov/GPO/LPS72661

http://www.homelandsecurity.org/newjournal/articles/tucker-israel.html

UNCTAD Secretariat—see United Nations Conference on Trade and Development Secretariat.


http://www.cbo.gov/ftpdoc.cfm?index=3277&type=1

http://www.cbo.gov/showdoc.cfm?index=5414&sequence=0

http://purl.access.gpo.gov/GPO/LPS60188


http://www.diw.de/deutsch/produkte/veranstaltungen/ws_consequences/docs/diw_ws_consequences200206_walkenhorst.pdf


http://www.rand.org/pubs/monographs/MG388/

http://www.rand.org/pubs/technical_reports/TR214/

http://www.rand.org/pubs/monograph_reports/MR1693/