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.

TECHNICAL
REPORT

Economically Targeted Terrorism

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

Brian A. Jackson, Lloyd Dixon,
Victoria A. Greenfield

RAND CENTER FOR TERRORISM RISK MANAGEMENT POLICY

The research described in this report was conducted within the RAND Center for Terrorism Risk Management Policy (CTRMP).

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

Summary

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, producing 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 exception 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 measures 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. 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.

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.)

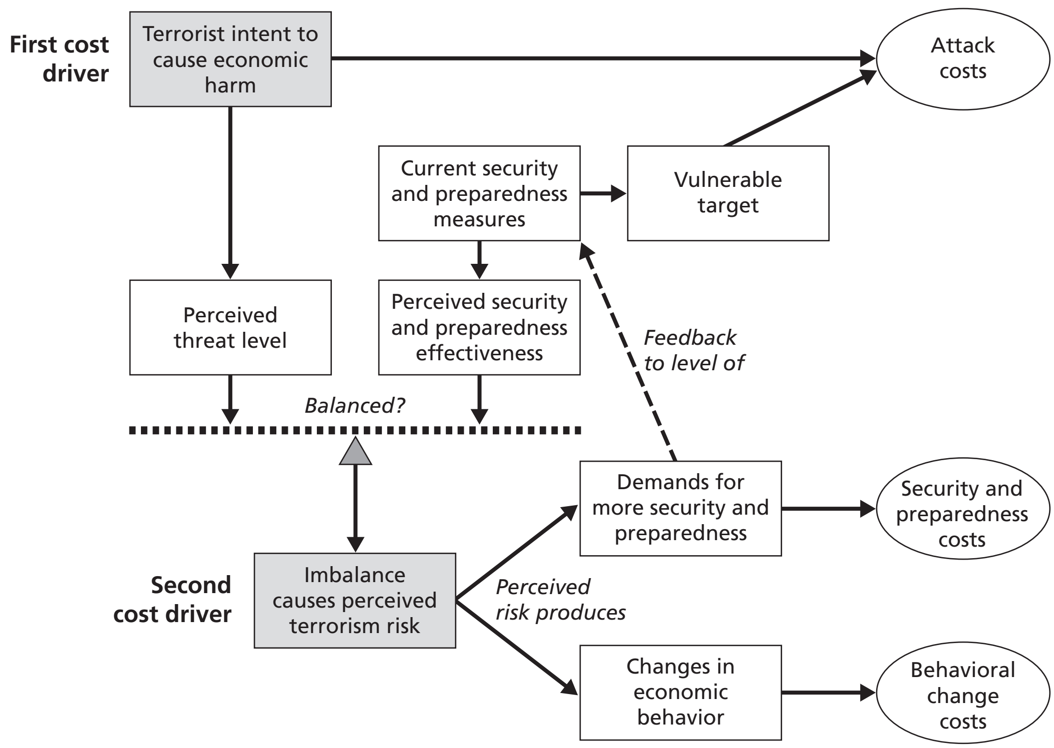
Defending Against Economically Targeted Terrorism

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



RAND *TR476-S.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.

We present four options that illustrate the range of tactics that might be used to apply these two levers:[3]

- *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.