1. Introduction

**Harry W. Richardson, Peter Gordon and
James E. Moore II**

This book is the second edited volume in a series about the economic consequences of terrorist attacks. The first was published in 2005, *The Economic Impacts of Terrorist Attacks* (Edward Elgar Publishing). It consisted (in addition to the Introduction) of 15 chapters by economists and others with expertise on terrorist issues, some but not all of them associated with CREATE (the Center for Risk and Economic Analysis of Terrorism Events) at the University of Southern California and sponsored by the US Department of Homeland Security. The book covered a variety of topics: transnational terrorism, air baggage security, electricity supply, biological attacks, homeland security communications, terrorist threat impacts on land values, container inspections, port security, radiological bomb attacks and destruction of bridges at the ports, the bombing of major highway bridges and modeling research (cost-benefit analysis and computable general equilibrium analysis). This volume returns to some of the same topics and some of the same authors, but also expands the range of both topics and authors.

Deterrence has been a crucial element in fighting terrorism. But in some cases there may be superior strategies to deterrence. In chapter 2, Frey and Luechinger suggest three policies, which could easily be compatible with the existing constitutions of democratic and rule-based countries. Two policies are based on diminishing the marginal benefit of terrorist acts for prospective terrorists. This can be done by decentralizing various parts of the economy or by diverting attention from terrorists, once a terrorist act has been committed. Another policy is to raise the opportunity cost, rather than the material cost, to terrorists. The effectiveness of positive incentives is substantiated by a discussion of the peace process in Northern Ireland and an overview of the empirical literature on the relationship between terrorism and political freedoms.

The Kunreuther and Michel-Kerjan chapter (chapter 3) focuses on the Terrorism Risk Insurance Act (TRIA) passed in 2002 as a temporary measure to increase the availability of commercial coverage for terrorist

acts. The chapter discusses terrorism risk insurability in the context of homeland security with a focus on the design of TRIA and impediments to free markets for terrorism risk management, including state regulation. The chapter attempts to measure the impact of TRIA loss-sharing from a terrorist attack by victims, insurers, all commercial policyholders and taxpayers. It draws on two large data-sets: first, the premia and surpluses of the 451 largest insurance firms operating in the US property and casualty and workers' compensation markets; and second, scenarios of different types of terrorist attacks against 477 high-rise buildings in the country. The focus is on Los Angeles alongside comparisons with New York and Houston. The conclusion of the analysis is that taxpayers are unlikely to be liable for losses below \$15 billion. For a \$25 billion loss, insurers and policyholders would handle between 80 and 100 percent of the loss depending on the property take-up rate. Only for terrorist attacks where insured losses were \$100 billion or more, would taxpayers have to pay 50 percent or more of the claims.

Robert Poole argues in chapter 4 that the legislation that created the Transportation Security Administration (TSA) and the current approach to aviation security, though well intentioned, was poorly thought out and is fundamentally flawed. It mandated costly changes in some aspects of aviation security, without any analysis of relative risks, costs or benefits. Consequently, it has wasted passengers' time and absorbed large sums of money that could have done more to improve security if used in other ways. With recent changes in leadership at the TSA and its parent agency, the Department of Homeland Security, the time is ripe for rethinking how the USA approaches airport security.

There are three basic flaws in the current model. First, the law presumes that all air travelers are equally likely to be a threat, and mandates equal attention (and spending) on each – which is very wasteful of scarce security resources. Second, the TSA operates in a highly centralized manner, which is poorly matched to the wide variation in sizes and types of passenger airports. Third, the law puts the TSA in the conflicted position of being both the airport security policymaker and regulator, and the provider of some (but not all) airport security services.

Department of Homeland Security Secretary Chertoff has repeatedly called for reorienting security policies along risk-based lines. At the same time, the General Accounting Office has found that today's very costly airport screening is little better than what existed prior to 'federalization' of this function. Also, the performance-contracting approach implemented on a pilot program basis at five airports appears to have worked slightly better than TSA-provided screening. Both factors set the stage for fundamental reform.

The chapter calls for three major reforms to address the three key flaws in the current approach. First, to remove the inherent conflict of interest, the TSA should be phased out of performing airport screening services. Instead, its role should become purely policy-making and regulatory (and better balanced among all transportation modes). Second, the screening functions should be devolved to each individual airport under TSA oversight. Third, screening and other airport security functions should be redesigned along risk-based lines to target resources better on identifying dangerous people rather than dangerous objects.

Devolving screening responsibilities to airports would mean that each airport could decide to meet the requirements either with its own workforce or by hiring a TSA-approved screening contractor. This model has been used successfully in Europe and Israel since the 1980s, and has worked very well. Funding would be reallocated to airports on a monthly (or at least quarterly) basis, rather than annually as at present. This would permit a much better match of screener numbers to actual passenger throughput in the rapidly changing airline environment.

If the funding was managed at the airport level, airport managers would have strong incentives to finance the upgrading of baggage-screening systems to make them less labor-intensive. At most larger airports, this would mean replacing lobby-based EDS (explosive detection systems) machines with automated, in-line EDS systems. At smaller airports, it would replace labor-intensive ETD (electronic trace detection) installations with EDS machines transferred from larger airports. These changes alone would save over \$700 million per year in screener staffing costs nationwide.

A risk-based model would separate passengers into three groups: low-risk, high-risk and ordinary. Low-risk travelers would be those who qualify for Registered Traveler status. They would get expedited checkpoint processing and their bags could usually bypass EDS screening. This change would cut future EDS acquisition costs by \$1–2 billion, and would yield another \$200 million annual savings in baggage screener costs. High-risk travelers would receive mandatory body-scans and explosive-detection inspection of both checked and carry-on baggage.

These changes would free resources to use for increased security in lobby areas and on the tarmac, as well as improved control of access by non-passengers to secure areas. Overall, this set of risk-based changes would put much greater emphasis on guarding against the threat of explosives (as opposed to just weapons) getting onto planes, as well as the threat of suicide bombers in terminals and on planes.

In addition, by putting all airport security functions under the control of the airport (instead of dividing them between the airport and the TSA, as today), and putting all these functions under arm's-length TSA regulation,

overall airport security would be more integrated and more effective, and the whole program would be more accountable. Freeing almost \$1 billion a year from screening would provide the resources for reconfiguring passenger checkpoints and beefing up the other aspects of airport security.

As the United States has regrouped in the years since the attacks of 11 September 2001, the question of how best to protect our cities from future acts of terrorism has been a topic of continuing discussion. However, despite a rational concern with terrorist vehicle-bomb attacks and other threat scenarios, a coherent, cost-effective strategy for protecting buildings and facilities while maintaining full and free access to them has yet to emerge. As a result, building owners and managers have been forced to implement ad hoc approaches targeted more at generic vulnerabilities than at actual threats – not necessarily an effective, let alone cost-effective approach to urban terrorism. Richard Little's chapter (chapter 5) explores basic risk management principles as a means for building owners, alone or in groups, and in partnership with municipal and federal authorities, to develop responses that balance actual threats, available resources, and a consensus level of risk tolerance.

Onur Bakir analyzes in chapter 6 how the risks posed by the import of illegal weapons and explosives to launch attacks in the US homeland have grown significantly in recent years. Sea borders remain vulnerable because it is very costly to inspect every vessel that sails in American waterways. He examines the inspection strategies that the United States Coast Guard (USCG) should adopt, given the level of risk and cost of operations that could deter commercial or personal vessel owners from collaborating with terrorists. The critical question is how the optimal strategy changes with respect to critical factors that affect the decision to collaborate with terrorists. Two cases are analyzed. First, all small vessels are assumed to pose the same level of terrorism risk. Some insights are provided into the impact of risk aversion on optimal strategy. He then extends the initial model to include two different risk types. The model shows that the USCG should allocate more resources to high-risk small vessels while maintaining some minimal level of deterrence on both risk types.

Larry Parkinson in chapter 7 examines the problems facing the Department of the Interior and the National Park Service (NPS) in protecting national iconic monuments (such as the Statue of Liberty, the Liberty Bell, the National Mall and the St Louis Arch) against terrorist attacks. Given that no extra security funds are provided, the NPS has to consider risks, threats and deterrence. The chapter uses the Statue of Liberty, the Liberty Bell and Independence Hall as case-studies of risk assessment and management. The key issue is how, under severe fiscal constraints, to draw a balance between security and freedom of access.

There is no universal solution because that balance has to be drawn in the context of the specifics of the individual iconic site, taking account of history, tradition, aesthetics, community preferences, budget constraints and symbolism.

Tom Stinson focuses in chapter 8 on the macroeconomic impacts of terrorist attacks. He does not consider the psychological and emotional consequences of an attack, but instead measures the direct economic losses (the value of the lives and income lost and the business activity lost by firms in the industries and communities directly affected by any attack) associated with terrorist actions. He suggests that although these losses can be catastrophic for the individuals and firms affected, and while substantial at the micro level, they are likely to be small when viewed in the context of the US economy as a whole.

The long-term impacts of a terrorist attack on the economy as a whole may be much larger than the direct losses associated with an attack. A modest slowdown in national consumer spending, a slight increase in interest rates, a brief slump in the stock market, and a small increase in the value of the dollar will all slow the US economy only slightly in the short run. But even a small, temporary decline in the growth rate in an \$11 trillion economy is likely to dwarf the direct losses caused by a terrorist act.

For example, in the long run, any future terrorist attack will require many firms to increase the resources they devote to security. Productivity losses will be very costly, even after appropriately discounting future reductions in output to present values, because the amounts lost will not be recovered over a few years but will continue to grow, uninterrupted, into the future.

This chapter is one of the first attempts to provide a measure of the scale of the national economic losses resulting from a catastrophic terrorist event. Its focus is on the broad, spillover effects of such an attack on the national economy, not on the direct losses suffered by the victims of the attack. The research was motivated by concerns about the impact of a major food terrorism incident, but the value assigned to the indirect economic loss estimates by this study is indicative of the indirect economic impact of other large-scale, catastrophic terrorist events. The chapter analyzes six real-world attacks occurring after 1970. Three were major events: the 9/11 aircraft hijackings that led to the destruction of the World Trade Center's Twin Towers; Iraq's invasion of Kuwait in August 1990; and the Iranian Embassy hostage situation which began in October 1979. Three were lesser events: the original World Trade Center bombing attempt in February 1993; the Embassy bombings in Africa of July 1998; and the attack on the USS *Cole* in September 2000. He uses these examples to predict the five-year macroeconomic impact of a hypothetical attack occurring in 2005.

A terrorist act of the scale hypothesized would also create significant losses at the personal, firm and industry levels, but those losses were outside the scope of this analysis. No adjustments are made to reflect the value of the lives lost or the direct losses suffered by economic sectors. Estimates of the productivity losses which may follow attacks, almost certainly larger than the short-term indirect losses estimated, were also not included.

Matthew Drennan focuses in chapter 9 on whether shocks to local economies (in this case, New York City after 9/11) result in temporary or permanent dislocations. This question has received considerable attention since New York's experience of 9/11. His argument is that agglomeration economies are difficult to destroy but that they are more network- than space-based. After the destruction of the World Trade Center, the firms that had occupied one-half of the destroyed space of all large tenants chose to relocate elsewhere downtown despite the fact that they could have paid much lower rents by relocating across the river in urban New Jersey. Thus, the spatial advantages and the business networks linking downtown firms with each other, with midtown, the region and the world, were not eliminated.

Nevertheless, spatial advantages and place-specific business networks and agglomeration economies can be eroded because of changes in technology and shifts in national and international demand. Drennan uses the historical example of the flood of 1972 in Elmira, New York, to show that a negative shock to a stagnant economy can have a permanent effect. On the other hand, despite its relative poverty, Homestead recovered quite quickly from the effects of Hurricane Andrew in the 1990s, primarily because of its location within the dynamic metropolitan region of Miami. A question of some concern is whether the slow decline of New Orleans over the 25 years before Hurricane Katrina may imply that the adverse economic effects of the flooding could be permanent.

Hamid Mohtadi and Antu Panini Murshid address a very different issue in chapter 10. Using a data-set constructed about terrorist activity involving the use of chemical, biological or radionuclear (CBRN) agents, they calculate the likelihood of a catastrophic event of this nature. Assuming a continuation of recent trends in the use of CBRN agents, an attack of the same magnitude as that on the Tokyo subway in 1995 could be expected to occur by 2009. Consistent with pronounced non-stationary patterns in these data, the 'reoccurrence period' for such an attack decreases every year. Similar trends are evident in a broader data-set which is non-specific as to the methods or means of attack. For instance, an attack that results in the deaths of 1000 people could be expected to occur within the next ten years. However an attack of the same magnitude as the September 11 tragedy, when nearly 3000 people died, is not expected in the near future.

Relying on a wide array of data sources, Park et al. specify and apply an operational multi-regional input–output (MRIO) model for the United States in chapter 11. The National Interstate Economic Model (NIEMO) provides results for 47 major economic sectors (called the ‘USC sectors’, developed to reconcile these models and all the different databases) for all 50 states, the District of Columbia, and a residual (or leakage) region, ‘The Rest of the World’. NIEMO is used to estimate industry and state-level impacts from the short-term loss of the services of three major US seaports – Los Angeles/Long Beach, New York/Newark and Houston – as a consequence of terrorist attacks. The attacks on the three port complexes are treated as alternatives rather than as simultaneous events. A one-month loss of the services of the Los Angeles/Long Beach port costs the US economy approximately \$21 billion. Corresponding impacts for the ports of New York/New Jersey and Houston are \$14.4 billion and \$8.4 billion, respectively. State-by-state impacts are a function of state size and distance from the site of attack.

Richardson et al. also use the NIEMO (National Interstate Economic Model) model in chapter 12 to trace the interregional economic effects of attacks on major theme parks (11 individual parks plus two geographical clusters) located in a modest number of states (eight). The theme parks are identified by state but not by smaller geographical units, to avoid identifying individual parks. A key assumption of some of the major scenarios is that an attack on one theme park will be perceived as an attack on all (this is called ‘spillover’). However, the chapter also examines a more conservative assumption, that an attack on one park will not affect attendances at others. It also takes account of the probability that even a major terrorist attack on a theme park will not eliminate American vacations, but rather result in shifts to safer destinations. One possible scenario is examined: substituting visits to national parks for theme parks.

The results are easily summarized. In the spillover cases, the range of estimates of business interruption is between \$19 billion and \$23 billion plus up to \$12 billion of air revenue losses. Without spillovers, the impacts are much smaller, between \$500 million and \$11.3 billion. These numbers combined may be in the same neighborhood as the costs of the 9/11 disaster. In diversion scenarios (for example, substitution of national parks for theme parks), there are economic losses because some people will stay at home, increase their savings and postpone decisions. Of course, there are offsets. In the national parks example, Florida and California are net losers (despite having important national parks), while states such as Arizona, Utah and Wyoming gain.

The economic impact estimates in this study certainly justify more expenditures on prevention. The problem is in spillover scenarios: how can

the smaller theme parks afford the costs of more prevention? Perhaps the answer is a combination of local, state and/or subsidies and a co-insurance scheme among theme park owners.

The last four chapters deal with interruptions to electricity supply as a result, either explicitly or implicitly, of a terrorist attack. However, the virtue of protections for the electricity system is that they have a dual function. Not only do they guard against or mitigate terrorist acts they also protect against natural disasters, weather-related events and massive equipment failure.

Lester Lave and his colleagues point out in chapter 13 that the American economy and our lifestyles are dependent on reliable, low-cost electricity. Unfortunately, natural hazards and human error frequently leave us in the dark. Blackouts cost the economy billions of dollars and threaten health and safety. Parts of the electricity system are highly vulnerable to attack. The combination of high cost of disruptions and extreme vulnerability has led disgruntled workers, environmental extremists and landowners to target the electricity system. Paradoxically, there is an important side benefit from the facts that natural hazards and human error have posed major challenges to the electricity system; the efforts to reduce the disruption and to speed recovery from these challenges have made it easier to cope with a terrorist threat.

With thought and design, major steps can be taken to accomplish simultaneously improvements in reliability and protection of the system against natural hazards, human error and human attack. The chapter stresses the importance of interactions among the three types of threats since the benefits of improving any one might be too small to justify taking action, while the benefits of mitigating the effects of all three threats might generate several times the benefit of any one and justify taking action. In particular, recognizing the interactions among the three may easily justify steps to improve the reliability of electricity delivery beyond current levels.

The general goal is to improve the resiliency of the US electricity system. The chapter explores 11 ways of enhancing resilience: improving operator training and communication; developing multiple transmission lines for service delivery; erecting physical barriers for protecting key substations; diversification of fuel supply and generation technology; on-site fuel storage; decentralized generation with intelligent control; automated distribution; back-up generators; promoting the ability to shed individual loads automatically; improved, secure information and control systems including the use of autonomous distribution agents; and building up the inventories of portable high-voltage transformers. Each of these approaches should be subjected to detailed cost-benefit analysis.

Rae Zimmerman, Carlos Restrepo and the rest of their research team (chapter 14) estimate the loss of service that might result from terrorist attacks on electric power grids using the New York City area as an exemplar scenario. The model is based on electricity interruptions resulting from factors other than terrorist attacks. The mean value of gross domestic product (GDP) for each American is estimated at \$112 per person per day, the social loss from a premature death used is US Environmental Protection Agency's (EPA) estimate (adjusted to current dollars) of \$5.8 million, and the value of time lost from transportation-related congestion resulting from a blackout is half the average wage. Using these parameters and combining them with outputs from a statistical analysis of outage events, the chapter estimates the losses from hypothetical blackouts caused by a storm or crime, and so on. For example, a winter blackout in New York that lasts 20 hours and affects 2.6 million people is estimated to cost \$245 million in business losses, \$870 million in death and injury, and \$117 million in congestion, resulting in a total loss of \$1.2 billion. Although these estimates are uncertain because the scenario is not defined in detail, the method can be used to estimate the social costs of a range of disruption scenarios from terrorist attacks on electric power for any other area of the country.

Adam Rose and his group (chapter 15) explore lifeline interruptions as a result of terrorism at the local level, more specifically water supply interruption in Los Angeles. The chapter develops and applies a computable general disequilibrium model to estimate the business interruption impacts of an attack on the water supply system serving Los Angeles County. The model has several attributes: it was especially designed to incorporate engineering and spatial aspects of the water supply system in the context of the regional economy, to reflect the several types of disequilibria that a water supply disruption would bring about, to include the various inherent and adaptive resilience responses at the individual, market and economy-wide levels, and to capture both partial and general equilibrium effects. The simulation of a two-week total water outage in LA County amounts to a business interruption loss of \$20.7 billion without any resilience adjustment, and \$2.3 billion with the inclusion of several types of resilience, most prominently the rescheduling (recapture) of production after water supply is restored. The results indicate that inherent aspects of the water–economy relationship (for example, input substitution) and adaptive behavioral responses (for example, conservation, water storage) can reduce the potential disruption impacts by 88 percent.

There are two key caveats to the analysis. First, many of the resilience factors are rough estimates, and more empirical work is needed to refine them. However, the model serves the useful purpose of identifying the

many important considerations affecting the impacts and the relative sensitivity of the results to these various factors. This provides a guide to setting priorities for further conceptual and empirical research. Second, the chapter measures only one, although likely the major, aspect of water supply disruption – business interruption. This result could be supplemented by crude estimating factors for household impacts, property damage and casualties. The next priority would be to extend the model to estimate household impacts, given the sizeable portion of the market represented by this customer group.

One final conclusion has a great bearing on future policy and is especially poignant in light of Hurricane Katrina. In the aftermath of the September 11 terrorist attacks, no politician wanted to admit that the government could not protect its people from a major threat. Likewise, in the case of utility outages, no matter what the cause, US citizens have looked to utilities to protect them. This chapter indicates how customers can protect themselves and contribute to the national war on terrorism by enhancing resilience to disasters in general. It identifies several ways this can be accomplished and the relative effectiveness of each type of resilience response at the individual, market and regional economy levels. There is a strong indication that people learn from disaster experiences, and that options implemented for one type of disaster apply to others (for example, purchase of back-up electric generators in the aftermath of the Northridge Earthquake). Thus, there is some cause for optimism that resilience to disasters will increase over time.

Richard Schuler (chapter 16) suggests that high-voltage electricity systems may become more reliable under market-based dispatch than they were under cost-based, regulated assignments if customers are faced with real-time prices. As an example, in Australia where all electricity is transacted through a spot energy market without any regulatory price caps, retail suppliers and large customers have installed frequency-sensing devices to turn off or reduce power to designated loads when the system's frequency falls below a pre-set level. While most of these relay installations were required by the grid managers, some of the automated load-shedding is also purchased as a market service. These mechanisms were put to the test in summer 2004 when the system suddenly lost 3100 MW of generation. Sufficient load was shed automatically so the system restabilized within 30 seconds. In periods when demand exceeds the system's supply capability, either because of unexpected high demand or supply disturbances, there is an inverse relationship between frequency and the price of electricity. So automatic load-shedding devices could also help buyers avoid price spikes.

While there is little experience in the United States with widespread direct customer participation in electricity markets, economic experiments have

been conducted at Cornell University with human subjects. These trials of full two-sided electricity markets are cleared subject to the laws of physics over Cornell's PowerWeb, 30 bus, 6 generator, simulated AC power network. The results demonstrate the ability of a small portion (20 percent) of active customers to mute the market power exercised by sophisticated players representing the generators, all without regulated price caps or strictures against withholding capacity. Furthermore, simulations of electrical flows on individual lines suggest that the capacity needs of the system per MW of overall demand are up to 10 percent smaller with active customer participation, compared to a regulated regime, and that would provide more breathing room for existing facilities. Those line flows are also more predictable when customers are actively engaged in power markets, making the job of dispatching and controlling the system easier. So if we want to reap the full benefits of markets for power in the US, including enhanced reliability and robust rapid responses to natural or terrorist-inflicted assault, we need to get the customers into the game as full participants.

A wide range of topics has been explored in this book, but there are many more being currently researched or to be addressed in the future. These include MANPADS (for example, portable rocket propelled grenade) attacks on airplanes, more attacks on downtown office buildings (using methods other than suicide aircraft bombers), terrorist-induced Foot and Mouth attacks on the animal population and other types of biological attacks (many of them impacting humans), more border security issues, and the mother of all attacks – a terrorist-based nuclear attack. Also, the close relationship between terrorist (that is, manmade) and natural disasters should not be ignored. By the time that this book appears, CREATE will have held a conference on the impacts of Hurricane Katrina. Lessons should be learned from that terrible event that will have repercussions for emergency response, prevention and other issues related to terrorism.