
1

WHERE PRIVATE EFFICIENCY MEETS PUBLIC VULNERABILITY

The Critical Infrastructure Challenge

*Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte,
and Erwann O. Michel-Kerjan*

2001: September 11 attacks. The theoretical vulnerability of the United States to a major terrorist strike is suddenly a stark reality. Impacts are global and enduring.

2003: U.S.–Canada blackout. A massive failure of the electric power distribution system demonstrates how human error can jeopardize vital public services.

2004: Indian Ocean tsunami. A deadly wave travels through Southeast Asian waters more quickly than potentially life-saving warnings through air-waves. Nearly 300,000 lose their lives.

2005: Hurricane Katrina. Four years after the 9/11 attacks, a violent but long-anticipated hurricane overwhelms a vulnerable coastline, meets an unprepared government, and inflicts lasting damage on a population. A superpower fails to meet the most basic needs of its citizens in crisis.

Are these recent disasters related? Will coming years bring ones even more severe? Is our modern, highly interconnected, global economy creating new types of vulnerabilities and worsening old ones? Who can act to reduce these vulnerabilities – in particular, to prevent terrorist attacks and natural disasters from having catastrophic consequences? More to the point, who *will* act?

This book contributes to the current and long-overdue debate on these questions. A series of important recent reports and studies sound the alarm on the inadequate preparedness of government at all levels to cope with the new generation of challenges evidenced by the crises listed above; the reports of the 9/11 Commission and of the congressional committee investigating the government's actions during and shortly after Hurricane Katrina are particularly

notable.¹ This book focuses on the private sector's role, will, and capacity in reducing public vulnerability to disasters. The book addresses public policies that would make the impacts of extreme events less severe and that would facilitate recovery after they occur. We do not offer definitive answers. We do show, however, that on many critical points relating to extreme event preparedness and recovery, conventional wisdom is wrong.

Conventional wisdom holds that, in the aftermath of the 9/11 terrorist attacks and the Madrid terrorist bombings on March 11, 2004, among numerous others, national governments around the world are working closely and effectively with relevant private enterprises to minimize the probability and impact of future attacks. They are not.

Conventional wisdom holds that federally backed insurance markets for catastrophic risks currently help induce private firms and households to invest in reducing the public's vulnerability from high-impact events. They do not.

Conventional wisdom holds that people base their decisions on how to prepare for extreme events on rational expectations regarding relevant probabilities. They do not.

Conventional wisdom holds that catastrophic terrorism, natural disasters, or inadvertent failures of large-scale public services are so distinct from each other that they should be addressed and managed separately. They are not.

Conventional wisdom holds that federal, regional, and municipal governments are able to reduce the likelihood of catastrophic events, and that the power to ensure recovery from such events occurs rapidly. They have neither.

The twenty-first century is not the twentieth. In almost every part of the world, economic life today is far more institutionally decentralized than it was 50 years ago, at the height of the industrial age. In developed countries, the infrastructure that provides essential services to citizens is more complex and interconnected by orders of magnitude than it was even a generation ago. In the United States, more than 80 percent of the shopping malls, office buildings, theaters, factories, energy installations, and airlines – all of which are potentially the subject of attack or natural disaster – are owned by private businesses.² Even though transportation facilities, such as airports, bridges, dams, and tunnels, are typically owned by municipal, state, or federal authorities, the planes, trucks, railcars, and ships that use these facilities are privately held.

Private actors seeking to increase competitiveness through greater operational efficiency will normally outsource, automate, or eliminate tasks viewed as peripheral to their core business competency, and they will avoid investing in equipment viewed as redundant. To reduce costs, managers may seek ways to make use of external infrastructures for which others bear the cost – as in the case of any firm using the Internet as the backbone of internal corporate communications. They may undertake to reduce redundancy in internal systems,

and decrease depths of protective “fire walls” to levels consistent with “normal” levels of risk.³ Other actions, including mergers and acquisitions, may be aimed at realizing economies of scale and scope – improving corporate performance by embracing a wider range of functions and opportunities.

Distributed efforts to improve productive efficiency at the firm level have yielded countless improvements, the cumulative effect of which over past decades has resulted in staggering reductions in costs. Yet competitive pressures do not allow firms to make large investments aimed at reducing vulnerability to disasters that are highly unlikely and nearly impossible to predict. Just as the industrial age exposed environmental vulnerabilities as an economic and social reality, so the post-industrial age in which we now live is in the process of exposing a different set of vulnerabilities: the “endogenous” security vulnerabilities of civil society.

FACING A NEW ERA OF ENDOGENOUS VULNERABILITIES

What makes a public vulnerability endogenous? Simply put, an endogenous event is one for which the outcome is at least in part the result of human actions. Hurricane Katrina is a good example. The hurricane damage was magnified first by the failure of the system of levees and barriers protecting the city of New Orleans, and second by the failure of the public officials responsible for protecting its people – for example, the collapse of communications systems and the absence of security protocols enabling infrastructure-service providers to reach affected areas. An “exogenous” counter-example is a meteor strike: This event is completely the result of actions beyond human control.⁴ Until recently, hurricanes and other extreme weather events were similarly viewed as exogenous events (described, in the language of faith rather than of economics, as “acts of God”). However, we increasingly understand that not only the impacts of extreme events, but actually the probability of their occurrence, are affected by human actions – cumulative decisions that weaken natural barriers to storm surges, place human populations in vulnerable areas, and change environmental and climate patterns on a global scale. In millennia of human history, this is new.

The abstract concept of an “endogenous security vulnerability” is thus everywhere present today in the brick-and-mortar world of everyday business decision making. Moreover, the increasing race for competitiveness and economies of scale calls for the development of larger systems, with larger potential associated risks. Many examples exist of large-scale and/or highly connected infrastructures vulnerable to events in which the probability of occurrence is low, but consequences when they do take place are severe: athletic facilities holding

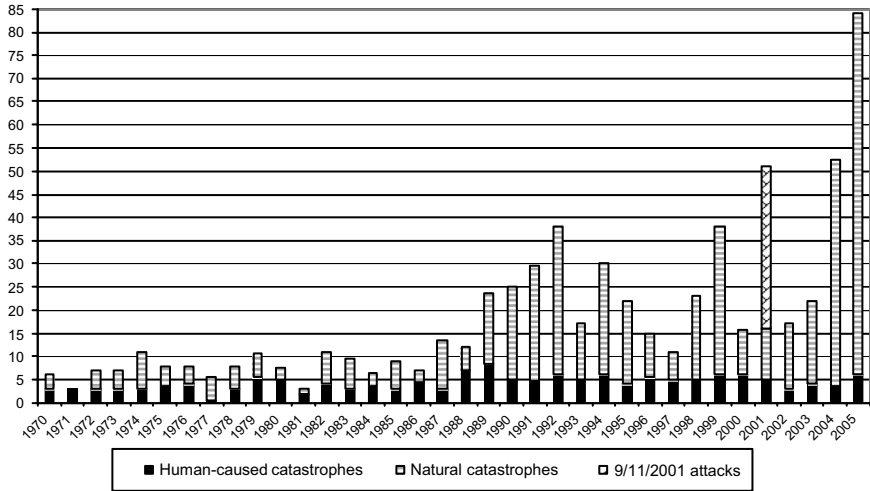


Figure 1.1. Natural and human-caused catastrophe insured losses, 1970–2005 (in US\$ billions).

100,000 persons, aircraft like the new Airbus 380 seating up to 850 passengers; food processing and distribution firms serving ever increasing shares of the national market; power distribution networks serving a third of the nation's population; and a new Royal Caribbean cruise liner that will carry 6,400 vacationers. In each of these examples, the quest for economies of scale induced by a highly competitive market economy has potential to amplify the consequences of a catastrophic failure in an infrastructure system. At the same time, as was evidenced in the aftermath of Hurricane Katrina, the efficient practices of private firms subject to market discipline have the potential to be significant assets in a time of crisis.⁵ Both increased vulnerability and a potentially increased capacity to respond are natural outcomes of the competitive process in decentralized market economies.

Of course, this business reality does not explain everything. The nature and spectra of potential risks have evolved as well. The recent occurrence of particularly destructive natural disasters raises the question as to whether there are now more natural catastrophes than before. Figure 1.1 illustrates that economic losses due to natural disasters worldwide have increased significantly over the past 25 years. Adjusted for inflation, the combined natural and human-caused insured losses were \$5 billion annually in the 1950s, \$8 billion in the 1960s, \$16 billion in the 1970s, \$22 billion in the 1980s, and on average \$70 billion annually in the 1990s.⁶ The annual increases continue to accelerate. In 2004, the total financial losses attributed to natural disasters around the world were

\$120 billion. In 2005, Hurricane Katrina alone caused even higher losses, with the exact total still unknown as we go to press. Population growth and its rapidly increasing urban concentration (both in absolute and relative terms),⁷ the increasing value of assets,⁸ and the lack of adequate mitigation measures in hazard-prone areas have largely contributed to this totally new level of economic loss. Whether the natural phenomena in such highly exposed areas are becoming more intense is also an open question.⁹

In contrast with natural disasters, both the impacts of a terrorist attack and the probability of one occurring are directly affected by the actions of governments, businesses, and citizens. As the report by the 9/11 Commission documents, prior to the 9/11 attacks, the U.S. government did not adequately respond to repeated warnings or implement indicated policies to reduce the hazard.¹⁰ Government action occurs in a context where the nature of terrorism itself has also dramatically changed over the past 20 years. While the total number of international terrorist attacks worldwide has been significantly decreasing on average during the 1990s compared with the 1980s,¹¹ the number of terrorist attacks by extremist religious-based organizations has increased. Such terrorist groups have demonstrated a willingness to inflict massive casualties and to view civilians as legitimate targets. That focus has led over the past years to fewer attacks inflicting a considerably higher number of casualties.¹² The 15 terrorist attacks that inflicted the greatest number of casualties (fatalities and injuries combined) occurred after 1982, with two-thirds of them occurring between 1995 and 2005 (Table 1.1).

Terrorist groups such as Al Qaeda have publicly called for attacks that not only inflict massive casualties, but also create major economic disruptions. Thus, the nature of the target has also evolved over time. Traditionally, attacks have been aimed at government, military, and diplomatic targets. Today, most terrorist attacks worldwide are directed against private entities (80 percent of attacks against U.S. interests in 2000, 90 percent in 2001).¹³

As concerns about terrorist attacks have grown, private-sector executives and policymakers have grappled with far greater uncertainties than ever before. The uncertainties are compounded by the fact that potential attackers can engage in “adaptive predation,” in which they purposefully adapt their strategies to take advantage of weaknesses in prevention efforts. In contrast, actions can be taken to reduce damage from future natural disasters with the knowledge that only the consequences, but not the probability, of natural disasters will be affected by the adoption of protective measures. The likelihood of an earthquake of a given intensity in Los Angeles will not change if property owners design more quake-resistant structures. The likelihood and consequences of a terrorist attack, however, change over time and are determined by a mix of strategies

Table 1.1. The 15 worst terrorist acts since 1983, in terms of casualties

Date	Location	Event	Fatalities	Injuries
07 Aug 98	Nairobi, Kenya	Bomb attacks on U.S. embassy complex	253	5,075
11 Sep 01	New York, Virginia, and Pennsylvania, USA	Terrorist attacks using aircraft	3,000	2,250
11 Mar 04	Madrid, Spain	Bomb attacks on trains	192	1,500
31 Jan 96	Colombo, Sri Lanka	Bomb attack on Ceylinco House	100	1,500
12 Mar 93	Bombay, India	Series of 13 bomb attacks	300	1,100
26 Feb 93	New York, USA	Bomb attack in the World Trade Center	6	1,000
7 July 05	London, UK	Bomb attacks in trains and bus	57	700
19 Apr 95	Oklahoma City, USA	Truck bomb attack on government building	166	467
12 Oct 02	Bali, Indonesia	Bomb attack in a nightclub	190	300
23 Oct 83	Beirut, Lebanon	Bomb attack on U.S. Marine barracks and French paratrooper base	300	100
03 Sept 04	Beslan, Russia	Hostages killed	360	NA
21 Dec 88	Lockerbie, UK	Explosion of U.S. PanAm B-747	270	NA
18 Jul 94	Buenos Aires, Argentina	Bomb attack	95	147
23 Nov 96	Comoros, Indian Ocean	Hijacked Ethiopian aircraft ditched at sea	127	NA
13 Sep 99	Moscow, Russia	Bomb destroys apartment building	118	NA

and counter-strategies developed by a range of stakeholders. This “dynamic uncertainty” makes the likelihood of future terrorist events against specific targets all but impossible to estimate, increases the difficulty of measuring the effectiveness of public policies and private strategies, and severely complicates efforts to allocate resources.

NO CORPORATION IS AN ISLAND: BUSINESS STRATEGY AND THE ECONOMICS OF SECURITY EXTERNALITIES

Businesses may not always realize how their failure to operate could affect a large number of agents, often rippling far beyond their direct influence. This effect is partially because business entities responsible for initiating a cascading failure across multiple economic sectors are not likely to be held accountable for negligence. As a consequence, there is divergence between what economists refer to as “private costs” and “social costs” of the firms’ actions.

Private costs are privately borne; social costs are borne by the community. When both the costs and benefits of an action are privately borne, then there is every reason to believe that investment decisions to mitigate such costs will be privately optimal. However, when a private decision has social impacts, either costs or benefits, that are not taken into account by the private actor, then it is more likely that the outcome will not be optimal from a societal standpoint.

The classic example is environmental pollution. Factories have smokestacks to remove smoke from the workplace. Unless compelled (e.g., by government) to take into account the damage to people by the smoke emitted outside the plant, the manager of the factory will treat the cost to the community of emission to be zero. Smoke in this instance is an example of a negative “environmental externality” resulting from a private decision – the smoke is sent outside the factory, and thereafter is no longer considered to be the manager’s problem.

This book develops broadly, and in new contexts, the concept of a “security externality.”¹⁴ In the case of a security externality, a private firm undertakes an action that creates a vulnerability (or possibly an uncompensated benefit) elsewhere in the economy. For example, if an electric power distribution firm buys only one very large, ultra-high voltage transformer, it minimizes its own expenses, but it also increases overall vulnerability. If that transformer has no replacement, and if it is attacked, the cost of service interruption will be distributed to all segments of society. On the other hand, if the firm provides technology that allows the damaged transformer to be replaced quickly, the increased assurance of reliable power, even in a terrorist attack, represents a positive security externality.¹⁵ The trade-off between private efficiency and public vulnerability emerges from the existence of security externalities (see Box 1.1). The challenge for public policy is to find a way for the government to provide incentives to the private sector to invest adequately in security (including both technical designs and management practices).

ENSURING THE DELIVERY OF CRITICAL INFRASTRUCTURE SERVICES: EMPHASIS AND ORGANIZATION OF THE VOLUME

The influence of private action on public vulnerability is a broad issue. This book focuses on concrete ways that highly industrialized democracies can better face future disasters or avoid them. Indeed, in a world of limited resources, not everything can be protected. To illustrate the broader concepts, as well as to contribute to a particular policy debate of vital importance, we concentrate on the challenges associated with the protection of society’s critical infrastructure of economic networks and public services whose continuity in times of disaster

BOX 1.1 CSX RAILROAD AND THE DISTRICT OF COLUMBIA

Less than a month after a January 2004 train crash in South Carolina resulted in the release of deadly chlorine gas that killed 9 people and hospitalized 58 others, the district's City Council passed an act banning the transportation of hazardous materials within a 2.2-mile radius of the U. S. Capitol without a permit. The act cited the failure of the federal government "to prevent the terrorist threat." Subsequently, CSX petitioned the U.S. Surface Transportation Board (USSTP) to invalidate the legislation, claiming that it would "add hundreds of miles and days of transit time to hazardous materials shipments" and adversely affect rail service around the country. USSTP ruled in CSX's favor in March 2005, putting an end to the district's efforts.

Shortly after the decision, Richard Falkenrath, President Bush's former deputy homeland security advisor, highlighted in congressional testimony the severity of the threat that the act was intended to address: "Of all the various remaining civilian vulnerabilities in America today, one stands alone as uniquely deadly, pervasive, and susceptible to terrorist attack: toxic-inhalation hazard (TIH) of industrial chemicals, such as chlorine, ammonia, phosgene, methylbromide, hydrochloric and various other acids."

The case of CSX Railroad and the District of Columbia illustrates the tensions that have emerged recently between two potentially competing imperatives: corporate efficiency and public security. Despite the urgency created by terrorist threats, as well as the ongoing challenges of dealing with natural disasters, a public-private consensus on how best to address these tensions has not emerged.

is critical to the economic and social continuity of a region, a country, or even a continent.

For at least as long as roads, bridges, and cities have existed, the reliable operation of infrastructure has been a concern of both rulers and merchants. Yet the infrastructure challenges faced by government and business leaders a hundred or even fifty years ago are primitive in comparison with those we must address today. Public policy must address three sources of low-frequency, high-consequence disasters: natural disasters such as hurricanes, floods, and earthquakes; "technogenic" disasters resulting from bad system design, inappropriate regulatory frameworks, and political and managerial failure; and disasters created by terrorists (domestic or foreign) and any other malevolent actors who can purposefully adapt their strategies depending on the security measures we take. The long-established but non-rationalized system of regulatory agencies intended to protect public safety in food, transportation, nuclear energy, oil and gas, and chemical plants, among others, today must function alongside new tools for protecting those same assets from terrorism. The failure of all levels of the U.S. government to properly prepare to mitigate the damage and manage the crisis in a timely fashion during and following Hurricane

Katrina has demonstrated in stark terms how far the United States still has to go in meeting these challenges.

How did the United States get to where it is today? Approaches toward “infrastructure” policy have evolved over the past century, from an initial emphasis on infrastructure adequacy, through deregulation with the aim of increasing efficiency through competition, to a recent focus on infrastructure protection. At the beginning of the 1980s, the national debate was driven by concern over the poor physical condition of public works infrastructure. In a report to Congress on the condition of national infrastructures released in 1983, the Congressional Budget Office focused on seven infrastructures that “share the common characteristics of capital intensiveness and high public investment at all levels of government. They are, moreover, directly critical to activity in the nation’s economy.”¹⁶ These seven infrastructures were highways, public transit systems, wastewater treatment works, water resources, air traffic control, airports, and municipal water supply. In its 1988 report to the President and Congress, the National Council on Public Works Improvement (created in 1984) defined infrastructure as systems providing services that “form the underpinnings of the nation’s defense, a strong economy and our health and safety” (see Box 1.2).¹⁷

By the early 1990s, policymakers’ attentions had largely moved away from broad infrastructure issues. Instead, legislative proposals tended to address the economic needs of individual infrastructure sectors, reducing regulatory

BOX 1.2 CRITICAL INFRASTRUCTURE SECTORS

The President’s National Strategy for Homeland Security issued on July 16, 2002, identified 13 sectors of the economy as comprising the “critical infrastructure” of the United States:

- Agriculture
- Food
- Water
- Public Health
- Emergency services
- Government
- Defense Industrial Base
- Information and telecommunications
- Energy
- Transportation (people and product)
- Banking and Finance
- Chemical Industry
- Postal and Shipping

constraints to allow infrastructures to increase their efficiency and lower the cost of service through more open competition.

An important turn was made in 1996, however, with the establishment by President Clinton of the President's Commission on Critical Infrastructure Protection, chaired by General Robert Marsh (the author of the foreword to this book). With the work of the commission, the security dimensions of public policies relating to infrastructure began to gain a weight equal to efficiency conditions. During the decade that has elapsed between the publication of the recommendations by the Marsh commission on critical infrastructure protection and the publication of this book, a series of government-commissioned studies have called attention, in tones of accelerating urgency, to the threat of terrorism and the necessity of government action to forestall it. These studies, and the government actions in both statute and executive orders, are detailed by authors in Part II.

Each time the government has attempted to redefine a complete list of critical infrastructures, the list has grown longer.¹⁸ At present, it includes not only operational public service networks such as energy, agriculture, transportation, and communications, but also a collection of "framing services" such as the defense industrial base and public health. This increase in the number of critical infrastructures suggests that a thoughtfully constructed model of the U.S. economy – or that of any technologically sophisticated, free-market democracy – comprises a network of enterprises providing products and services that are highly interdependent. To the extent these interdependencies look like externalities to the managers of each enterprise, and are not fully under their control, the function of this network becomes an unavoidable concern of collective institutions, of which the most comprehensive in its coverage is government. Government regulatory agencies find themselves engaged with almost all the nodes of this largely private interlocking network of infrastructure service providers.

The broader list of interdependent infrastructures also illustrates the range of relationships that exist between governments at different levels and firms engaged in critical service provision – from government corporations such as the U.S. Postal Service to self-regulated sectors such as the chemical industry. In open, democratic societies, protection from the most severe impacts of rare but high-consequence disasters is not the responsibility of government alone. Indeed, the greatest cost of an excessive focus on failures by government entities may be the missed opportunity to encourage more effective action and engagement by private entities.

In this volume, we explore four categories of action toward the aim of ensuring the delivery of critical services: managing organizations, securing networks, creating markets, and building trust.

MANAGING ORGANIZATIONS

In protecting against massive disruptions of critical services, the responsibility for setting goals rests primarily with the government, but the implementation of steps to reduce the vulnerability of privately owned and corporate assets depends primarily on private-sector knowledge and action. Although private firms uniquely understand their operations and the hazards they entail, they currently do not have adequate commercial incentive to fund vulnerability reduction. A few industries, notably nuclear power generation and air traffic control systems, succeed in operating complex and hazardous systems with extraordinarily high levels of reliability, even in the face of extreme stress or system turbulence. These organizations fail so much less often than their normal counterparts that they serve as potential models for all critical infrastructure systems, where society requires services, to the extent possible, to remain functioning against a very wide range of threats and disruptive conditions. To the extent that effective response capabilities can be transferred, or learned, they may prove invaluable to other industries facing disaster risks. However, for reasons stated above, private firms will resist making changes for security reasons that will deeply affect organizational practices. These issues are discussed in Part III.

SECURING NETWORKS

In the presence of interdependencies, even if each firm is resilient, the system may still be vulnerable due to lack of coordination among, and communication between, different industry sectors. As companies build and manage systems with greater reach and higher capacity, they find that those systems are also increasingly linked to other large, technical systems. The use of large-sized networks and their interconnections allow firms to reduce their operating cost, thanks to economies of scale. System engineers have made considerable progress in increasing the reliability and robustness of large service networks at the same time that they have increased their efficiency. The ability of Toyota not only to build and deliver a new car of a particular configuration requested by a customer, but to do so in two weeks, provides additional customer value and attests to the efficiency of Toyota's supply chain. But if parts supply is interrupted, there is very little buffer to sustain production. The complexity and global reach of supply chain networks make them vulnerable to disruption. When the large-scale networks provide critical services, the impacts of their failure are felt widely and immediately. "Cascading" effects may result in the failure of other systems. All of these impacts may be rendered particularly severe if damage is due to deliberate destruction. These issues are discussed in Part IV.

CREATING MARKETS

Various informational and coordination problems have led many to believe that the best solutions are market based. Yet little evidence exists to support the claim that market forces alone are sufficient to induce needed investments in protection. Over the past few years, senior executives and federal officials have begun to view insurance as a market-based tool to address public vulnerabilities. The fact that insurers are private-sector actors tends to facilitate communication with other private firms, avoiding concerns about relationships with federal agencies. Insurers are recognized as risk management experts, and it is in their own interest to limit the exposure of their clients. In theory, the pricing of insurance coverage can be used to induce investments in vulnerability reduction. Yet serious questions exist regarding the extent to which insurance (including reinsurance and access to new financial instruments to cover catastrophic risks) and other market-design mechanisms can actually prove to be a significant tool in ensuring the provision of critical services. Private capital alone may not be able to cover large-scale risks that may reach into the tens – if not hundreds – of billions of dollars, while continuing to provide coverage for more traditional risks we all face in our day-to-day life. Firms – both insurance firms and the businesses they protect – face increasing difficulties estimating the probability of an attack occurring tomorrow and evaluating the consequences. And being insured might also induce private actors to reduce, rather than increase, investments in vulnerability reduction. How might firms at risk assess their vulnerability and identify the technical and managerial measures to mitigate that risk? These issues are discussed in Part V.

BUILDING TRUST

The challenge facing both business and government leaders is not only to balance public and private interests, but to understand the way in which these interests are intertwined. As the number of identifiable infrastructure sectors continues to rise, and their interdependencies evolve in a mesh network of relationships, the public interest takes on a large number of varied forms. How, then, can a collaboration between private interests and government be characterized as a balance to be struck across a single political table? Indeed, how can such a model be applicable to the international cooperation that is also required? A new model of joint public–private collaboration must evolve if there is to be a sustainable, efficient, and robust economy in the face of threats of many kinds. Every catastrophe threatens to destroy the one element most required for response and recovery: trust. These issues are discussed in Part VI.

“We reflect on the 9/11 Commission’s finding that the most important failure was one of imagination,” wrote the members of the House Committee investigating the response to Hurricane Katrina in their final report. “The Select Committee believes Katrina was primarily a failure of initiative. But there is, of course, a nexus between the two. Both imagination and initiative require good information. And a coordinated process for sharing it. And a willingness to use information – however imperfect or incomplete – to fuel action.”

This volume offers an array of insights into how, in a competitive market economy, operational practice, business strategy and public policy can jointly ensure the reliable provision of infrastructure services. Together, these insights serve to direct attention away from the infrastructure itself, and toward the institutions, incentives, and behaviors that have created – and are constantly re-creating – that infrastructure. While there are no easy solutions to the challenges we describe, our final chapter addresses the unavoidable necessity for a more effective public and private collaboration on the provision of critical services and the reduction of public vulnerability. Just as a previous generation of policymakers adapted to the emergence of environmental externalities, policymakers today must adapt to a world in which security externalities are suddenly ubiquitous. Yet to address the new challenges that we highlighted at the outset, improved public policy and business strategies will not be enough. Action requires imagination and initiative – in other words, leadership.

NOTES

1. The National Commission on Terrorist Attacks Upon the United States 2004; Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina 2006.
2. President’s Council of Science and Technology Advisors 2003, p. 15.
3. Many examples are cited in National Research Council 2002b on the structure of networks and their vulnerability to attack, see Albert et al. 2000.
4. Posner (2005) discusses a variety of catastrophes, including the one that would be caused by a large meteor hitting the earth. That case illustrates a catastrophe in which human actions could mitigate impact, but not the probability of an event occurring.
5. For illustrations, see testimony provided to the U.S. Senate Committee on Homeland Security and Governmental Affairs in November 16, 2005, hearing titled “Hurricane Katrina: What Can Government Learn from the Private Sector’s Response?”
6. Data from Munich Re.
7. In 1950, about 30 percent of the world’s population – 2.5 billion people – lived in cities. In 2000, about 50 percent of the world’s population (6 billion) lived in cities. Projections by the United Nations show that by 2025, that figure will have increased up to 60 percent of a total 2025-population of 8.3 billion people. This results in the increasing number of “mega-cities,” with populations above 10 million. In 1950, New York City was the only

- such mega-city. In 1990, there were twelve such cities. By 2015, there would be twenty-six, including Tokyo (29 million), Shanghai (18 million), New York (17.6 million), and Los Angeles (14.2 million), just to name a few located in hazard-prone areas.
8. For example, if Hurricane Andrew had occurred in 2002 rather than 1992, it would have inflicted double the economic loss, mainly due to increased coastal development and rising asset values located on the coasts of Florida.
 9. See Michel-Kerjan et al. 2006. The 2005 hurricane season exceeded the 1933 record for the busiest season since hurricane counting started in 1851 (23). Evidence suggests that the Atlantic Ocean may be entering a cyclical period of more intense storms, and it possible that ocean warming associated with climate change may exacerbate this trend.
 10. See, for instance, Enders and Sandler 2000, pp. 307–332; Sandler and Enders 2004, pp. 301–316; Hoffman 1998; Chalk et al. 2005.
 11. U.S. Department of State 2004.
 12. Pillar 2001; Wedgwood 2002; Stern 2003.
 13. U.S. Department of State 2004.
 14. The concept of security externalities as employed by the editors of this book is a generalization of the concept of interdependent security discussed by Heal et al. in Part IV of the book on securing networks.
 15. This example is discussed in National Research Council 2002b, pp. 180–195.
 16. U.S. Congressional Budget Office 1983, p. 1.
 17. National Council on Public Works Improvement 1988, p. 33.
 18. In the 2003 *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Office of the President, 2003, p. 7, the notion of “key assets” was introduced. Among these are “national monuments, symbols, and icons that represent our nation’s heritage, traditions, and values and political power. . . .” These are doubtless important targets for terrorists, but are not addressed in this book because they do not constitute elements of critical infrastructure. The Homeland Security Presidential Directive 7 issued on December 17, 2003, adopts the same critical infrastructure and key assets that are in the 2003 National Strategy.