

---

# 26

## LEADERSHIP: WHO WILL ACT?

### Integrating Public and Private Interests to Make a Safer World

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

---

*“To be courageous . . . requires no exceptional qualifications, no magic formulas. . . .  
It is an opportunity that sooner or later is presented to us all.  
The stories of past courage can define that ingredient, –  
they can teach, they can offer hope, they can provide inspiration.  
But they cannot supply courage itself. For this each man must look into his soul.”*

John F. Kennedy, *Profiles in Courage*, 1956

At the outset of this book, we asserted that the combined efforts of the government and the private sector have not adequately reduced the public’s vulnerability to catastrophic terrorist attacks, natural disasters, and other low-probability, high-impact events. Contributors to this volume have discussed five elements of a coherent and complete response: evaluating vulnerabilities, managing organizations, securing networks, creating markets, and building trust. The effectiveness of each depends on the execution of the others. Yet none will develop without a sixth element: sustained commitments carried out through effective leadership.

By “leadership” we do not mean the political image of a charismatic individual able to mobilize action through sheer force of personality (although that is a valuable, albeit rare, attribute). Rather we mean the assumption of responsibility and accountability by individuals with sufficient authority over resources and decisions to effectively address catastrophic events. As many studies document, however, the reality of an immediate response to a disaster is overwhelmingly unplanned, decentralized, and the product of private action – “leadership” on a micro-level, perhaps, but not at the scale of national policy.

Public policy leadership is most essential when decisions involve difficult trade-offs between collective and private interests; it is only *expected* when those trade-offs are widely understood. Leadership, in the absence of such

understanding, lacks legitimacy. When disasters do occur and “obviously” important objectives are not achieved (as was the case in New Orleans during and after Hurricane Katrina), it is usually because leadership responsibilities have not been adequately defined or exerted to address these trade-offs.

This book has focused on building awareness about a specific category of trade-off in a complex industrial society: private efficiency versus public vulnerability. This balancing act is well understood in highly industrialized, democratic, market economies. Firms in the private sector are encouraged (by market rewards) to maximize their productivity by cutting costs and increasing efficiency. But their behavior is constrained by an extensive body of government regulations and administrative and legal institutions that interpret and enforce them. Public health for consumers and workers, honest and ethical market behavior, and protection of endangered resources in the natural environment are all values that citizens and consumers seek through collective action by their government. But these protections are usually assembled slowly and through an elaborate give-and-take between public and private political interests.

An acceptable and sustainable set of rules is only achieved when the risks to the public and the requirements of a strong economy are in balance. When the severity or timing of risks are not predictable, the democratic process is unlikely to balance the interests without controversy. An example is the accumulating scientific evidence that dependence on fossil fuels is irreversibly changing the earth's climate. However, neither the pace of change nor its specific consequences in all local regions are yet widely enough accepted to force political acceptance of the economic costs of acting before those consequences have been widely experienced. (On a positive note, see Box 26.1 for a recent example of CEO-level initiative).

The potential for catastrophe, especially as caused by terrorists who may act deliberately and creatively to inflict large-scale damage, poses a challenging dilemma for society: How can the collective interest in reducing risks of high-impact, though low-probability, future events be balanced against the immediate certainty of costs to be incurred by individuals – managers, investors, and consumers – to increase watchfulness, enhance the capacity to manage under extreme stress, and otherwise minimize the consequences of catastrophe?

In this volume, we have used the term “security externalities” to refer to risks in the management of a business enterprise that radiate out to others. Even when taken in sum, the contributions to the volume have not addressed all types of security externalities. We have not considered all categories of catastrophe, notably leaving aside human-induced climate change and other potential seeds of disaster extremely slow in their realization.<sup>1</sup> We also have not considered all sectors of the economy, focusing rather on the provision of those services essential to economic and physical well-being. Private firms bear

**BOX 26.1 DAVOS–G8 CLIMATE CHANGE ROUNDTABLE**

The World Economic Forum's G8 Climate Change Roundtable was launched at the forum's 2005 annual meeting in Davos, Switzerland, in response to an invitation from U.K. Prime Minister Tony Blair. The group was composed of chief executives from 24 global companies across a diverse set of industry sectors, including energy, air transportation, automotive, banking, metals and mining, and insurance. The roundtable's primary mission was to provide the Prime Minister with the business community's perspective on the climate change agenda for the 2005 G8 summit in Gleneagles, Scotland.

After a series of meetings and workshops between January and June 2005, the group presented Prime Minister Blair with a detailed set of recommendations affirming the importance of the problem—calling for a long-term, globally consistent policy regime involving all major emitters of greenhouse gases, and emphasizing the need to implement performance-based technology incentives. Acknowledging the risks to business posed by future regulation and/or climate-induced damage to assets, the group stressed the need for clear and consistent “price signals” to stimulate businesses to act.

Although the formal discussions of climate change at Gleneagles were disrupted considerably by the terrorist bomb attacks on the London Underground, the roundtable appears to have succeeded in demonstrating widespread support for properly designed mitigation throughout the global business community. The roundtable also helped create a broader context for engaging participation of key developing countries such as China, India, and Brazil in subsequent talks on climate change policy. Most importantly—by demonstrating widespread support for mitigation—the roundtable played an important role in helping shift the debate from “whether climate change is a problem” to “how the problem should be solved.”

most of the responsibility for the day-to-day provision of critical infrastructure services. Yet responsibility for the reliability, continuity, and resilience of the infrastructure that provides those services is shared with government.

Chapters 1 and 4 describe the multiple attempts by the U.S. government to define the critical infrastructure challenge. The U.S. government well understands *what* needs to be done, and *why*. Its policy—Homeland Security Presidential Directive 7 (December 17, 2003)—is clear: “The Department of Homeland Security (DHS) is responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States [and] leading, integrating, and coordinating efforts to protect critical infrastructure and key resources with an emphasis on those that could be exploited to cause catastrophic health effects or mass casualties.”<sup>2</sup> However, the nation will remain unnecessarily vulnerable until deeply divided responsibilities for its protection are reconciled, resulting in a shared understanding

of *how* to identify and mitigate vulnerabilities and *who* will assume leadership. If obligations, separate and joint, are not clearly laid out and accepted, then shared responsibility may end up being no responsibility at all.

## HOW WELL IS U.S. CRITICAL INFRASTRUCTURE PROTECTED?

What is the state of leadership in the United States with regard to vulnerability reduction and the provision of critical infrastructure services in times of disaster? Most agree that vulnerability is high and action is imperative. Box 1.1 in Chapter 1 provides an illustrative case of tensions between private efficiency and public vulnerability. At issue in that case, involving the District of Columbia and CSX Railroad, were chemical hazards. The magnitude of the challenge posed by this single risk category is enormous: a 2003 report of the U.S. Environmental Protection Agency indicates that there are 123 large chemical facilities in New Jersey alone where a release of chemicals could threaten more than a million people.<sup>3</sup> At the time the report was released, former Senator John Corzine asserted that DHS, the Justice Department, the Environmental Protection Agency, and industry groups such as the Chemical Industry Council were in accord that the issue must be addressed, but could not agree on who should be responsible for what actions.

The chemical industry successfully lobbied against passage of Senator Corzine's bill, the Chemical Security Act of 2003 (S. 157), preferring its own voluntary industry standards for safety and security. Congress, while failing to pass S. 157, did pass unanimously on July 14, 2005, a resolution calling for mandatory federal standards. The standards were not enacted. But in a speech on March 21, 2006, DHS Secretary Michael Chertoff reversed the administration's opposition to mandatory regulation of the chemical industry and supported legislation to require all 15,000 plants that use or store significant quantities of toxic chemicals to prepare security plans and follow up with steps such as fencing, cameras, and identification cards to control access. Thus, the main thrust was to prevent access, not to cause investments to reduce the inherent vulnerability of the plants.

Critics noted that because large firms already comply with most of what the administration proposed, the legislation's main effect is to extend those practices to smaller firms and make them mandatory. Secretary Chertoff also said that the nation should have uniform standards, strongly implying that states should not be allowed to adopt their own rules, as New Jersey did last year, particularly if those rules were more stringent than the federal government's.<sup>4</sup> It is widely understood that the chemical industry has consistently resisted

---

actions that would affect its profitability, which is understandable given that it is a low profit-margin business.

On the other hand, safety records of the largest chemical firms are good. The industry as a whole most likely has the competence to perform much better technically than it lets on. We argue that the safety standards in the chemical industry, including the more general hazard-related issues of chemical substitution, facility siting, transportation routing, and industrial interdependency, should not be determined by the lowest safety performers in the industry, which appears to be the case today. Leadership, both in the private sector and by government, is necessary to orchestrate movement away from the lowest common denominator when it comes to critical infrastructure performance and protection.

Firms will be reluctant to go beyond the proposed legislation and unilaterally invest heavily to reduce their own vulnerability if the industry lobbies effectively against legislation that would require its competitors to do the same thing. A more serious problem arises when the federal government intervenes to prevent state and municipal governments from taking stronger measures to safeguard their own communities against the risk of toxic chemical releases that could kill thousands of people.

If industry itself is not motivated to invest in protection against extreme events, and if the federal government does not take the initiative, who will take responsibility for protecting chemical plants, rail lines, hospitals, telecommunication systems, and other critical services? Who will make it harder for terrorists to magnify the damage of an attack by first attacking the infrastructure on which effective response depends? Who will ensure that these and other elements of the infrastructure are not used as weapons to kill or maim thousands of people in our cities? If they succeed, who will still trust the operation of our own critical services?

The lack of progress toward a well-defined balance of responsibilities between government and industry is illustrated by the proposed second version of the U.S. National Infrastructure Protection Plan (NIPP).<sup>5</sup> The NIPP constitutes a new step in the federal effort to protect the nation's critical infrastructure. This plan has recently been proposed by the government after extensive inter-agency negotiation led by DHS. The complexity of the task of coordinating roles of federal agencies alone is illustrated by the astonishing number of such agencies involved (see Figure 26.1).

This diagram represents all of the U.S. federal agencies with specific missions in Homeland Security and Homeland Defense.

The U.S. government recognizes that the great majority of the economic assets and the firms providing critical infrastructure services that are likely to



be severely damaged in a disaster are owned by private enterprises. The NIPP document lays out architecture and principles for the many tasks that need to be addressed.<sup>6</sup> But while this plan addresses in detail the roles of all relevant federal agencies, it does not address adequately the critical issues analyzed in this book, including the incentives that would best enhance the willingness of firms to organize and invest in reducing them, while preserving a fair and efficient competitive market for their services.

In fact, the revised NIPP devotes only two pages to the roles and responsibilities of the private sector from the firms' perspective.<sup>7</sup> Nevertheless, the NIPP is replete with emphasis on "security partnerships," implying a broadly understood and accepted set of agreements between government and private firms about how private and public sector institutions will collaborate.<sup>8</sup> In concept, partnership is appealing. The concrete practice of partnership is another matter. Indeed, partnership raises fundamental questions of control, responsibility, coordination, information sharing, liability, trust, and cost sharing, among others, that still need to be addressed by government bodies in charge of protecting the country and by the firms that will bear the financial and managerial burdens of implementing that level of protection. Among the issues that remain to be addressed are:

- How responsibility and accountability are to be apportioned between government and industry;
- What obligations each side will have to share sensitive or proprietary information with each other;
- Who will monitor the performance of each party, and what criteria for evaluation will they use;
- Who will provide the resources required for addressing the security externalities, including organizational reliability, that each side believes the others should cover;
- Who will be held liable after the next disaster, and to what extent;
- How will economic losses be compensated and who will pay for them;
- Up to what extent will taxpayers and consumers (and investors) be willing, over an indefinite period into the future, to pay for increasing public security.

These are challenges that call for a national infrastructure protection plan in which the private sector has a major voice and a major responsibility, and under which critical infrastructure businesses can be held accountable for whatever obligations to partner with government – and with other firms – they undertake. Not only does the first version of the NIPP fail to answer these difficult questions, but also it does not propose a venue within which the negotiation about them can be carried out.

---

## ROOTS OF RESPONSE: SEVEN FINDINGS TO INFORM ACTION

This book describes a complex set of threats to the safety and security of the United States, and indeed of other industrialized democracies. The potential severity of threats to critical infrastructure services is growing. At the same time, the public will demand a higher level of reliability and resilience in infrastructure services as they become more important in the economy. Yet as the requirements for addressing both of these trends grow, solving these problems becomes more difficult. The construction of the institutional relationships that will lead to enlightened decision making and actions will require an unusual degree of forward-looking leadership from both public and private sectors, and a deeper understanding on the part of the public of what is at stake.

Discussions regarding high-impact event preparedness and response almost inevitably feature actions recommended for immediate implementation. A number of these actions have been raised in this book. Equipping private- and public-sector first responders with interoperable communications equipment would at least make it possible for the response to the next major disaster to be more coordinated than was the response to 9/11 and Hurricane Katrina.<sup>9</sup> Issuing universally recognized identification cards to both public-sector and private-sector first responders (notably including infrastructure operators) would allow access to affected areas for all whose actions are required for recovery. Enacting legal provisions in each state to permit governors to suspend temporarily certain statutes if they impede necessary measures to deal with the emergency would reduce routine bureaucratic obstacles to response and recovery. Seeking to distribute federal grants to states and cities in proportion to the risks they face would introduce a minimal level of rationality to the process of public investment in vulnerability reduction.

In the United States in particular, a frustrated public can rightly ask: Why, five years after the September 11, 2001, attacks, and a full year after the Hurricane Katrina calamity, have these simple actions not been undertaken, even when demanded and funded by Congress? How severe does a disaster need to be before it motivates government into action?

The sentiment is a valid one. As Stephen Flynn emphasized in Chapter 3, the need for enhanced preparedness is urgent. Yet, if the many diverse contributions to this volume share one insight, it is that there are no technological quick fixes to the challenge of ensuring the reliable provision of critical services. Without forceful leadership from above and/or exceptional initiative from below, required organizational adaptations will not occur, and needed investment investments will not be made.

We believe that a set of ideas, actions, and policies must be accepted before the United States (and other countries) will respond in a concrete and timely

way. This set includes (1) adopting new models for dealing with the new scale of disasters; (2) integrating all-hazard strategies; (3) restructuring management practices and technologies; (4) providing clear incentives, knowledge, experience, and tools; (5) recognizing that perceptions of risk may be as important as their reality; (6) understanding the critical roles of insurance and reinsurance in the recovery process and its capacity to provide incentives for investment in infrastructure protection; and (7) acting with a clear recognition that interdependence is a multinational issue.

Policies and concrete collaborative actions may follow more easily if these seven actions are taken.

### **1. THE SCALE OF DISASTERS IS GROWING: A NEW ERA CALLS FOR A NEW MODEL**

Natural disasters, technological risks, and terrorism threats have always existed in one form or another. But society faces a new scale of these events today and, as we have argued, even more so tomorrow, because of increased aggregation of people and assets exposed to risks, along with the emergence of new forms of threat. As world population grows, people are flocking to cities and to coastal areas; larger numbers of individuals become exposed to a given catastrophic risk. And as incomes rise, the value of assets rises. As the economy grows, firms seek ever-larger aggregations of assets in the quest for economies of scale. With increased global economic integration, disasters reach across national boundaries with increasing frequency. As the scale of damage and death from disaster grows, it becomes necessary to prepare for ever-less-probable but increasingly consequential events.

The Gulf of Mexico has always suffered hurricanes. Hurricane Katrina, a widely predicted Category 3 storm when it made landfall on August 29, 2005, was not, however, just another hurricane. The large-scale hurricane damage, combined with the breach of New Orleans levees, became a major disaster. Preparing to deal with a local and limited event is one thing, but coping with a new dimension of loss and destabilization is another. One cannot simply apply the same evacuation rule for a million and a half people in four states as one would for a city of 50,000. A single event that, on top of several historically devastating years, inflicts insured losses for catastrophe lines equal to one- or even multi-year insured losses worldwide is not the same as numerous small independent events dispersed over 120 countries.

With economic and social activities concentrated in a limited number of areas, this new scale has to be seriously integrated into a new way of making important decisions. These extreme events will not simply require a little more of what we have previously learned, but a radical change in how to tackle them. A new scale calls for a new model.<sup>10</sup>

## 2. AN INTEGRATED STRATEGY FOR ADDRESSING DELIBERATE, NATURAL, AND TECHNOGENIC DISASTERS IS NEEDED

As discussed in Chapter 1, disasters are essentially of three types: natural, technogenic, and terrorist-caused. These three sources of possible disaster may also be interdependent or occur in combination. While it is critical to recognize the fundamental differences among these disasters and to respond appropriately when need be, the management policies and resources for mitigation and response to dealing with each of them have much in common.

This commonality is particularly apparent in the capabilities and tools of emergency first responders. The mission of the Federal Emergency Management Agency, now a part of DHS, is based on the assumption that this is so. It is widely acknowledged that Hurricane Katrina would have been much less damaging to New Orleans and the Gulf Coast if the destruction had not been compounded by technogenic and poor management amplification (badly engineered levees and barriers, growing populations in hazard-prone areas, poor post-flood response by local, state, and federal governments). In some cases, such as the spread of toxic chemicals in a railroad switchyard, first responders may even be forced to make decisions before they know if the event was accidental or the deliberate act of a terrorist. Thus, strategies intended to address all three – the “all hazard” strategies – need to be addressed by a comprehensive plan that responds to all three types of disasters and their combinations in the most efficient and sustainable way.

Likewise, firms can establish preparedness capacity (evacuation, business interruption issue, liability protection) to be used for all three types of catastrophe. Doing so would show how considering all hazards together spreads costs over a wider range of contingencies, making them more attractive economically than measures devoted to only one.<sup>11</sup>

We support a more sustainable national effort to reduce the danger and consequence of disasters based on the “all hazards” approach, in which investments in vulnerability reduction, continuity of operations, and preparation for recovery for all three types of disasters can, at least to some extent, be shared.

Sustainability of a national effort to reduce infrastructure service vulnerability to high-consequence terrorism may falter if too many years pass without a major catastrophe of a specific type. This is one of the reasons that an “all hazards” approach to infrastructure protection is required. Sustainability may also be threatened if effective protection depends on a level of international cooperation that proves not to be forthcoming.

But the most important element to enhance sustainability of the public commitment to vulnerability reduction is a strategy – industrial, technological, and regulatory – that searches for *dual* benefits (reduced vulnerability *and*

better service) from the public and private investments in the effort. Indeed, if one focuses only on the security aspect, it is likely that the short-term return on investment will not be seen as significant enough; but if benefits of better service are included as well (as it should be), then the strategy is immediately viewed as much more appealing. If the public becomes aware of such benefits, and if industry can find and profit from them, a more sustainable effort will be achieved. Some examples of service benefits are improved public health services (for both the normal health needs of communities and faster response to natural threats such as SARS and avian flu), environmental protection, less frequent contamination of the food supply, more reliable electric power and other services, less frequent delays in transportation systems, safer chemical and energy industries, improved defense against hackers and virus attacks, better tracking and billing of goods in transit, and reduced risk to fire, police, and emergency health professionals.

As industry looks for both new technologies and new management methods to reduce the costs of increased reliability and resilience and searches for additional service benefits that can help offset rising costs, the incremental cost to government of preparing for terrorism or unlikely natural disasters may also be reduced. For example, the government investment of \$7 billion in preparation for a bird flu pandemic that has yet to occur may also be a valuable step in anticipation of a biological attack, which has not yet occurred either.

### **3. INCREASINGLY INTERDEPENDENT SERVICES REQUIRES RESTRUCTURED MANAGEMENT PRACTICES AND TECHNOLOGIES TO MAKE THEM MORE RELIABLE AND RESILIENT**

High-tech market economies, such as in the United States, are increasingly turning from product manufacturing to integrated provision of services, which in combination with products and services, deliver consumer value most effectively. Given the accelerating rate at which manufactured products are driven to commodity production by competition from high-skilled, “low-ware” firms located abroad (e.g., India and China), the trend toward the increasing share of the economy devoted to provision of services is being driven by economic necessity as well as the quest for greater market satisfaction. The most critical of these services are normally delivered by an increasingly complex web of interdependent infrastructure services operated by the private sector, with highly variable (and generally diminishing) degrees of public regulation or direction.

The government’s current list of 13 critical infrastructures is only the tip of the iceberg of interrelated critical services. In fact, as discussed in the early part of the book, the government’s list continues to grow. Closer examination of

regional economies would show a fractal-like structure of networks of service firms in collaboration and competition with one another, each generating security externalities that require a collective response in the public interest. Thus, sustaining the reliability and resilience of this mesh network of infrastructure services is increasingly vital to economic and social life of the nation.

On the demand side, civil life has become more dependent on increasingly interdependent infrastructure services. As we have noted, because their interdependencies tend to increase the level of consequence when large-scale failures do occur, the public will demand higher levels of reliability, even in the absence of either natural or terrorist-initiated disasters. This demand will certainly be exacerbated in the aftermath of every disaster the country may face in the coming years.

The public's expectations, however, cannot be fully realized without government action in concert with the relevant industries. The public will demand that both private and public institutions make themselves accountable for high levels of service and security. This demand will grow stronger as vulnerability of critical services to both natural and deliberate disasters increases. How this demand will materialize is not clear today. Customers who want more reliable services will have to be willing to pay the price, and both public and private officials will have to be willing to be accountable.

On the supply side, executives of infrastructure service businesses are generally successful in managing to limit the service and financial consequences, in degree and duration, of statistically predictable interruptions in service from natural causes such as hurricanes or floods. They are well organized to deal with the many minor disruptions with which they have experience, and some even offer level-of-service guarantees. But they are increasingly faced with the possibility of less-predictable disasters, not only from terrorism but from decreased resilience of their operations. Firms with experience in providing highly reliable services, such as telephone and financial services, have developed management disciplines that are driven by a long-term commitment to operational goals and that have come to possess the organizational practices, management cultures, and external support needed to sustain them.

The advice in Part III details the essential practices, procedures, and structures that enable firms to manage the unexpected and transform a highly industrialized but loosely coupled economy to one much less vulnerable to high-consequence disasters. But very little attention, except in the most highly regulated industries such as nuclear power, has been given to public policies that might induce more critical infrastructure firms to restructure their management practices, policies, and organization to make them more resilient.

That might not matter if it were not for the fact that, as a general rule, the competitive drive for efficiency results in loss of reliability and resilience in

critical services. The urgency associated with public fears of a repeat of 9/11 has induced a very short-term view of critical infrastructure vulnerability. But the threats from nature, terrorists, and human failings will be with us for the indefinite future. Restructuring a highly industrialized economy to reduce not only the threats but the consequences of disaster is likely to be time-consuming and costly. We conclude that the very success of a competitive economy with a strong capacity for innovation may be changing the inherent vulnerability of critical infrastructure systems. Indeed, in many instances, there seems to be a direct but inverse correlation between success at driving business performance to higher productivity and lower cost in “normal times,” and resilience in the face of a threat of possible disaster.

As a general rule, firms seeking to become more competitive still seek efficiency gains in economies of both scale and scope, in concentration of activities in a limited number of geographical areas,<sup>12</sup> in reduction of redundancy, in aggregation of resources and services, and in dependence on the services and products provided by other infrastructures. One example of this interdependence of special importance is the advent of just-in-time processes – all of which result in loss of resilience in the face of disasters for which the likelihood and consequences (including ripple affects on those not directly affected by the event) are difficult to quantitatively predict and integrate in day-to-day business decisions.

A key strategic challenge of the new risk era is, that “disaster times” seem to have become much more frequent these past years. If the trend continues and is reinforced, this increase will require a radical change in how demand and supply sides’ priorities are established and how resources are allocated between normal and disaster times.

#### **4. KNOWLEDGE, EXPERIENCE, AND TOOLS TO ADDRESS SECURITY EXTERNALITIES ARE REQUIRED TO ALLOW RISKS TO BE ASSESSED AND RESPONSES CREATED**

A main objective for senior executives is to reduce the impact of an untoward event on their firm’s operations, limit their legal responsibility, and facilitate a back-to-normal crisis management strategy. However, the impacts of executives’ actions on other infrastructure services are not often integrated in crisis decision making. The main reason for this lack of integration is the absence of both quantitative information and mechanisms for internalizing these external effects, whether positive or negative. For example, markets do not reward firms for assuring high-reliability service offerings in the event of very low-probability events. This lack of reward inhibits the adoption of high-reliability management methods.

The new dimension of extreme events directly affects the security externality component we define and discuss in the introductory chapter of this book. Beyond the lack of appropriate economic, social, or legal incentives, firms do not tackle the security externality issue adequately for several reasons. While some teams of technical experts in the national labs, in research institutions, and in industry have made progress in methods for evaluating enterprise vulnerability, this knowledge has not been widely tested or diffused. Strengthening the focus of responsibility for critical infrastructure protection in DHS appears a necessary condition, given the diffusion of responsibility in the government today (Figure 26.1). This lack of general knowledge, experience, and tools inhibits market forces from motivating infrastructure service firms to invest in vulnerability reduction to lessen the likelihood of rare, high-consequence events.

The existence of interdependencies that are not well understood may lead organizations to decide not to invest in their own protection because they know that the failure of others to take similar actions can harm them, even if they do make such investments. One valuable way to reduce risks due to interdependencies is to evolve interdependence into mutual support.<sup>13</sup> Moreover, with well-defined risks, it is possible to measure the effective return on investment of specific security/mitigation measures. When it comes to rare disasters, on the other hand, it is very difficult, if not impossible, to define a distribution of probability and to quantify all the direct and indirect effects of such extreme events. What cannot be measured in quantitative terms may be more difficult to support as a private strategy (see Chapter 17).

An appealing way to address the problem is via the establishment of business coalitions. Members of the coalition collaborate to support their decisions aimed at reducing interdependent risks based on the analyses of the whole group.<sup>14</sup> Knowing that all coalition members are acting the same way increases the willingness of each individual member to act as well. When a critical number of participating organizations is reached, others might decide to join, eventually leading to new business practices for all. The key is to find the pivotal few firms that will demonstrate leadership by acting first. The objective should be to find assessment tools for which firms and agencies can have sufficient confidence to justify corporate investments in vulnerability reduction and recovery capabilities, can measure their return, and can be rewarded by specific market mechanisms (e.g., higher prices paid by customers or limited liability).

## **5. LARGE-SCALE RISK MANAGEMENT MUST REFLECT PERCEPTIONS AND REALITIES OF RISK**

As catastrophic risks are difficult to quantify, estimates and decisions are more likely to be based on qualitative factors, and they may even be very subjective.

Although this volume does not specifically address the issue of risk perception, we recognize that it plays a key, if quiet, role. It generally is not effectively integrated in the development of private strategies and public policies to protect critical services. Yet the integration of risk perception is fundamental for the success of any program to deal with catastrophic risk management. Risk perception is concerned with the psychological and emotional aspects of risks, which have been shown to have an enormous impact on individual and group behavior. It is also important to know how this perception and its corresponding behaviors (investments in security, insurance protection, creation of new security-related markets, political behaviors) change over time.<sup>15</sup>

A particularly serious example of a potential difference between perception and reality of risks is the public alarm that seems likely to accompany a terrorist attack with a radiation dispersal weapon, popularly called a “dirty bomb.” Such a weapon does not involve the most terrible of weapons of mass destruction, that is, a nuclear explosive, but rather a chemical explosion of radioactive waste material. The general public is poorly informed about the dangers of given types of radiation sources, their rate of dispersion, and common sense ways of reducing one’s exposure. Panic is widely predicted in the event of such an attack, and the public may not be willing to reoccupy contaminated areas for generations.

One of the ultimate challenges in protecting critical sectors is the choice of specific allocation of resources, which are by definition limited. Therefore, it is crucial to understand the threats decision makers and the public perceive as being the most important and those that most need to be protected against. The natural tendency to fight the previous war, rather than anticipate and prepare for the next one, must not be underestimated. Focusing for four years on homeland security has led some to forget that the country remains vulnerable to natural disasters as well. A new terrorist attack on U.S. soil would certainly reshape the debate again.

#### **6. THE ROLES OF INSURANCE AND REINSURANCE IN DISASTER RECOVERY AND IN INVESTMENT INCENTIVES IN PROTECTION MUST BE DEFINED AND FACILITATED IN POLICY**

Well-defined market mechanisms have a major role to play in assigning responsibility and motivating action to ensure the reliable provision of critical services. Among the market mechanisms, insurance appears to be an appealing candidate. It is well known that, without proper design, the availability of insurance is as likely to blunt incentives for required investments as it is to sharpen them. Yet insurance has potential to be a powerful instrument. The insurance industry is the world’s largest when measured in terms of revenues. Insurance diversifies risks nationwide and internationally, and it can play a

fundamental role in financially protecting the nation. Insurance constitutes a potential nexus between risk assessment, risk mitigation, and risk financing. Insurers and re-insurers are often seen as experts in understanding risks. They are private-sector players who understand how markets operate, a quality most businesses are often reluctant to attribute to any level of government.

As we demonstrate in Part V, a well-functioning insurance infrastructure is also a critical service itself. The fact that the public sector participates in most disaster insurance programs in the United States and several other industrialized countries shows an implicit recognition by government of the critical role played by the insurance infrastructure. The government has often stepped in when insurers refused to cover such events alone. Because of this importance in managing risks across the whole society, we call for recognizing the insurance industry as a critical sector on its own, rather than including it under a broad banking and finance umbrella. Including the insurance industry as the 14th U.S. critical sector would allow a better understanding by the general public, the government, and other critical services of the strengths and limitations of insurance operations. It would also help society deal with challenges of how best to finance recovery from all types of disasters. Such solutions should encourage the development of better mechanisms to reward investments in security and risk mitigation, thus limiting the need for post-disaster federal aid. Long-term programs also need to take equity issues into account – those who cannot afford insurance should not be left behind.

Large disasters present, however, a set of specific characteristics that challenge insurance and re-insurance operations: difficulty in estimating and pricing risks with confidence, high correlation of risks, and potential for extreme consequences that create solvency problems, among others. On the demand side, one often observes low demand for insurance coverage even in exposed areas (except just after a catastrophe, when demand temporarily increases, often significantly).<sup>16</sup> To make insurance a more effective market-mechanism tool to enhance higher security, one would have to better align demand and supply.

The type of leadership we call for in this book is certainly highly needed in the area of insurance and reinsurance as well. The unprecedented series of extreme events in the past few years have more urgently raised the question of the roles and responsibilities of the public and private sectors in providing adequate protection to catastrophe victims, both people and firms. In fact, between 2001 and 2005, the record of the most costly year ever in the history of catastrophe insurance and reinsurance worldwide has been hit three times; three times due to disasters in the United States. If the country continues to file the vast majority of world insurance and reinsurance claims in the next few years (more than 85 percent in 2005), how long will reinsurers, most of them non-U.S. firms, continue to cover insurers against extreme events in the United States? What

maximum capacity will they be able to provide, and at what price? How will insurers react if they cannot increase risk-based prices they would charge in highly exposed states because of strong market regulations such as Florida?

If a major catastrophe were to happen next week, the question of loss sharing and financing the economic and social consequences would likely take center stage. In other words, how best should society finance extreme event losses? This question will not be solved overnight, but it must be addressed as a national priority. However, the current debate on the protection of critical service stays essentially focused on the *ex ante* aspect (physical and cyber protection), rather than a necessary dual *ex ante/ex post* perspective (physical, cyber, and financial protection).

Terrorism risk is a perfect illustration. Attacks in Madrid and London, among others, demonstrate that the United States and its allies remain prime targets for some terrorist groups. The American public and business enterprises deserve a robust national debate on a long-term program for dealing with terrorism risk financing. The fact that the Terrorism Risk Insurance Act was renewed on the literal eve of its expiration in 2005 does not signal the type of leadership one might expect from a country that places homeland and national security as a top priority.

## **7. INTERDEPENDENCE IS MULTINATIONAL: COLLECTIVE INTERNATIONAL ACTIONS MUST FORM AN INTEGRAL PART OF PREVENTION AND RESPONSE STRATEGIES**

Finally, as critical services are evolving and their scale of operation is becoming larger and more linked internationally, new collaborative initiatives by the United States need to be undertaken at the international level. In the case of manufacturing supply chains (see Chapter 16), the vulnerability to disruption is rapidly growing as economies become increasingly global. A major incident in the port of Rotterdam, Hong Kong, or Shanghai would have huge impacts worldwide. The challenge of increasing the reliability and resilience of national critical services would be only partially addressed if it is not considered in the context of effective multinational strategies. In today's world, the United States does not have the option of simply closing its borders to protect itself from external threat. The barriers posed by these borders are eroding due to more and more open networks of people and markets in a global interdependent world, resulting in foreign firms operating some of the U.S. critical services and U.S. firms operating these services in other countries.

Ten years ago, with the establishment of the Commission headed by General Robert T. Marsh (author of the foreword to this book), the United States was the first country to put the critical infrastructure challenge on its national policy

agenda. Other countries have followed more recently, and their government agencies and businesses are acting to protect their critical services at home as well. For example, the European Council in June 2004 asked the European Commission – representing 25 European countries – to prepare an overall strategy to protect critical infrastructure. In December 2004, the council officially endorsed the commission's initiative to launch its European Programme for Critical Infrastructure Protection, with the release at the end of 2005 of its first official document.<sup>17</sup> As of now, however, the debate on the actions needed in Europe is still in its early stages.

Japan, accustomed to major natural disasters and the victim of domestic terrorist attacks as well (e.g., the Sarin gas attack in the Tokyo subway in 1995), has long had an extensive and well-organized program of response capability. In addition, Japan has now initiated programs of scientific research on means to reduce vulnerabilities, which it is undertaking in collaboration with the U.S. Department of State and other federal agencies.<sup>18</sup> The U.S. government has diligently sought foreign cooperation to make its own protections more effective, for example, in container inspections in foreign ports and new U.S. passport designs with biometric security features. But there are also opportunities for the United States to energize its international collaboration in the broader strategies to make the multinational family of critical service providers more robust, reliable, and resilient. Here again, the private and public sectors need to work hand-in-hand.

One should expect that U.S. partners among market economy democracies would be eager to respond to such initiatives. A major destabilization in the United States could have impacts, direct and indirect, short- and long-term, far from American shores. Interdependencies work both ways. Thus, there is an opportunity for win-win situations in transnational negotiations. In this case also, it requires leadership, indeed, international leadership.

In today's global economy, assuring rapid and transparent exchanges of information and plans for coordinated action must also be international. How is this international collaboration to be achieved? Mechanisms such as were demonstrated by the postal operators of Europe and the United States in response to the crisis created by the 2001 U.S. anthrax attack (see Chapter 25) are a good beginning. They demonstrate that it is possible to learn and act on these issues, and to act at a large scale. These initiatives reinforced trust – a crucial element when collectively preparing to face the unknown. But enhanced international capacity for coordinated real-time operational response is also badly needed in other areas such as information, computer networks, telecommunications, energy, health, and transportation. It is imperative that similar collective actions are launched systematically after each major destabilization and by leading organizations in multiple sectors. Coordination is the only proven

way to lay the groundwork for arrangements that enhance each nation's ability to cope the next time. Some encouragement may be drawn from an important move over the past few years.

Economically focused international organizations have started addressing resilience issues from a multinational collaborative perspective as well. The former Secretary General of the Organization for Economic Cooperation and Development (OECD), in a September 2005 address in Beijing, clearly stated the OECD's position (Box 26.2). Recognizing the question of large-scale risks and disasters as a priority of its future action plan, the OECD Directorate for Financial Affairs is now developing a network of reflection, study, and recommendations regarding the new challenges associated with extreme events, both natural and human caused. A multi-year project will be deployed in the coming months and will constitute a natural venue for decisionmakers interested in the critical aspects of dealing with the new scale of disasters.

#### BOX 26.2 OECD'S SECRETARY GENERAL ADDRESS ON CATASTROPHE RISKS

"The OECD risk management work began four years ago when by making an assessment of OECD countries' capacity to deal with a range of major threats ranging from natural disasters and terrorism to health risks and cyber-attacks. Our conclusion from that wide-ranging study was that, in almost all aspects of risk management – assessment, prevention, response and recovery – our member countries were not well positioned to deal effectively with the scale and complexity of the risks of the twenty-first century, and that considerable efforts would be required to make improvements.

Modern-day societies and economies are complex and sophisticated, often with multiple jurisdictions. In OECD countries there is very rarely a single organization that can legitimately control the operations of all public and private actors in the event of a peace-time disaster. But it is precisely such structural and organizational difficulties that need to be overcome if our capacity for handling disasters effectively is to be significantly improved. In the case of international-scale disasters, coordination is the key. . . .

Governments must address these challenges quickly and comprehensively. Preparing for and managing these risks requires a comprehensive and coordinated approach. A piecemeal response will not work; as the American proverb says "It doesn't work to leap a twenty-foot chasm in two ten-foot jumps."<sup>a</sup>

– Donald Johnston, Secretary-General, Organization for Economic Cooperation and Development

<sup>a</sup> Johnston 2005.

The World Economic Forum (WEF) in Geneva, Switzerland, has also made large-scale risk issues a priority in its future action plans. Indeed, in 2005, it selected for debate one of the most important and intractable threats: anthropogenic climate change induced by greenhouse gases. Box 26.1 illustrates a concrete and detailed initiative launched in 2005 by the forum along with G-8 members and senior executives of a number of multinational firms.

A series of similarly focused initiatives would increase society's common knowledge and be viewed by others as a reason to act. These actions bring the type of leadership we described earlier to the international scene. More broadly, the WEF recently launched its "Global Risks Network." Its aim is to assess key current and emerging systemic risks to global business, to study the links between them for their likely effects on markets and industries, and to advance thinking about mitigation. The network was created in 2004 by the WEF in collaboration with Merrill Lynch. In 2005, Swiss Re and Marsh & McLennan joined, along with several faculty members from the University of Pennsylvania's Wharton School as advisors. The 2006 forum in Davos contributed to increasing the awareness of leaders in businesses, governments, universities, and nongovernmental organizations regarding the network and its activities.

These multinational initiatives could lead to a whole new way of managing large-scale untoward events. Perhaps the most encouraging feature of the OECD and WEF initiatives is their engagement of business leaders in conjunction with international political leaders. While neither of these organizations seems appropriate for the detailed negotiations of responsibilities and accountability that must be agreed to by both business and government in each country, they may serve to stimulate recognition of the high priority of this work.

#### HOW CAN A NEW CONSENSUS OF PRIVATE AND PUBLIC INTERESTS COME ABOUT? – A CALL FOR COLLABORATIVE LEADERSHIP

The response we seek in this book to risks of extreme events goes well beyond the task of first responders to a disaster underway or to tactical response plans of citizens and local governments. We look to a preventive strategy that avoids the crisis costs and damages that would arise from a society poorly positioned to mitigate disasters before they happen. This crisis avoidance requires more than plans; it requires changes in management structures and practices, in analysis of vulnerabilities and risks, and in some cases changes in technologies. It requires a greater degree of collaboration across critical service sectors and across national boundaries. The current institutional structures needed to undertake this task are not in place—they must be invented. Building these institutions into effective bodies will require a new and different kind of leadership.

---

Leadership – courage, we may say – will require decision makers in critical industry sectors and in governments to be willing to take a long view of the nation’s future, even at the expense of short-term economic gains (industry) and political needs (government). This long-term view must be addressed in a non-partisan, non-ideological way. If dialogue and decisions are to be effective, not only in the short-term but sustained into the future, new institutional mechanisms will be required. The assignment of responsibilities, resources, and accountability requires a venue for addressing public–private collaboration. It cannot be dictated by government, nor will it arise naturally from market forces.

We have argued that the private sector will certainly shoulder the burden of financing most of the capital investment and making most of the institutional improvements that provide high reliability and robustness to their parts of critical service. But the private sector cannot do this alone. It requires incentives beyond those currently existing in critical-sector markets, some perhaps from insurance, others from government. Public–private collaboration with governments at all levels, along with intergovernmental cooperation, will have to rise to a level that businesses and governments do not today enjoy.

Beyond this public–private duality, the triptych of business–government–citizen should be brought together more systematically. Indeed, in an open, democratic society the ultimate decision maker is the citizen, functioning as a consumer and as a voter. Civic engagement and consumer responsibility offer promise for sustainable solutions. On the other hand, consumer negligence and refusal to pay today the price for public peace and security would be a sad alternative. Indeed, public apathy and consumer disengagement from the aggregate impacts of individual decisions create the ideal terrain to nurture the seeds of ever more severe disasters.

Courage “is an opportunity that sooner or later is presented to us all.” We can each expect that our moment to assume private responsibility for public vulnerabilities will come in time. The best time to assume that responsibility is now. This book seeks the achievement of a safer, more secure world by guiding the leadership efforts of those who recognize collective action as a proven way to succeed and, most importantly, those of visionaries who share our belief that a better world can be created; for us today, and for our children and grandchildren tomorrow.

## NOTES

---

1. A dramatic if much less likely threat is that of a large asteroid striking Earth. We know this has occurred more than once in Earth’s history. Only collective action can be taken to deal with such a threat. See Posner 2005.
2. Flynn 2005a.

3. Stephenson 2005. The GAO quotes DHS estimates that there are 4,000 chemical manufacturing facilities that produce, use, or store more than threshold amounts of chemicals that EPA has estimated pose the greatest risk to human health and the environment (Government Accountability Office 2005d).
4. Lipton 2006.
5. Department of Homeland Security 2006.
6. "Designed to meet the mandates set forth in Homeland Security Presidential Directive 7, the NIPP Base Plan also articulates security partner roles and responsibilities, protective framework milestones, and key implementation actions required to support our national-level critical infrastructures and key resources (CI/KR) protection mission. It establishes the architecture for conducting operational risk assessment and risk management activities and provides processes for coordinating resource priorities and informing the annual federal budget process; strengthening linkages between physical and cyber, domestic and international CI/KR protection efforts; improving information-sharing and public-private-sector coordination; and integrating steady-state protection programs in an all-hazards environment." E-mail communication from the NIPP office at DHS, January 20, 2006.
7. DHS officials expect a series of sector specific plans to be published in the summer of 2006 that will address roles of private firms and government in specific areas of critical infrastructure. Private communication March 15, 2006.
8. In addition, the NIPP lacks guidance for firms concerning operational practices that would improve system resilience and robustness. There are a small but notable number of examples of such systems, most run by some form of public-private partnership involving federal agencies already, which could inform the national policy discussion; some of these have been discussed in this book. The widespread adoption of some of these practices would go a long way to reducing the vulnerability of major disruption from an extreme event.
9. For a discussion of the issues, see National Task Force on Interoperability 2003.
10. Lagadec and Michel-Kerjan 2005.
11. For example, many different insurance solutions exist in the United States to cover against different types of disaster. The National Flood Insurance Program, a public program, covers floods. Storms on the other hand, are covered mainly by the private sector; the distinction between these two types of covering parties in Hurricane Katrina has been the subject of a great deal of conflict between insurance companies and their policyholders. An international terrorism act on U.S. soil would be covered by the Terrorism Risk Insurance Act, a private-public program; but this program does not cover domestic terrorism. Other countries have made a different choice by providing "all hazards" insurance policies. Whether a comprehensive "all hazards" coverage program in the United States would be appropriate economically, socially equitable, and politically sustainable is a question worth studying in more detail. For a discussion on natural hazards, see Kunreuther 2006.
12. In the chemical sector, for instance, there are large concentrations of facilities in several regions (Houston, Texas, the Kanawha Valley in West Virginia, the Delaware Valley, and the Northern New Jersey/New York area). Major disasters in any of these areas could have significant spillovers for the entire economy.
13. See contributions by Brian Lopez in Part II.
14. There might be important anti-trust limitations, however.
15. For recent contributions, see Slovic 1993, 1999, 2000; Horch et al. 2001; Morgan et al. 2002; Pidgeon et al. 2003.

16. There might be several reasons for that: (1) Memories of prior losses tend to fade if no similar events have occurred recently; (2) Insurance is perceived as a bad investment – “I paid this policy for years, and I never suffered any damage, so I’m going to cancel it”; (3) Insurance is only one tool that people and firms can use to protect themselves financially – for example, publicly traded firms can diversify their exposure over all shareholders; (4) The temptation of some to expect the government to step in anyway in the aftermath of a disaster can reduce their willingness to purchase coverage.
17. Commission of European Communities 2005.
18. Branscomb 2004.

