From: *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan (eds.), New York: Cambridge University Press, 2006, 429-456.

24

SHARING THE WATCH

Public–Private Collaboration for Infrastructure Security

John D. Donahue and Richard J. Zeckhauser

Vital physical assets must be protected. But against what risks? And how? And by whom? And at whose expense? After the terrorist attacks of 2001, these questions were propelled from back offices into boardrooms and cabinet meetings. The way American society resolves such questions will reshape broad swaths of the economy for the foreseeable future.

Security can be provided by the public sector, the private sector, or some blend of the two. The separability of financing and delivery further multiplies the options. For example, protection can be provided publicly but funded privately (through special tax levies on affected industries) or be provided privately but funded publicly (through tax subsidies or direct grants), or with various mixtures of public and private provision and funding.

This profusion of alternative delivery models is not hypothetical. Property owners defend against fire risks in part through private responses – alarms, extinguishers, sprinkler systems, fireproof materials – and in part through reliance on publicly provided fire fighters. Public police forces and private security services co-exist – although in the United States, the private force, in the aggregate, is larger (around a million private security guards, as of 2003, compared with about 600,000 police[1]) – and dividing lines can blur, as when public police officers moonlight for private clients. Airline security arrangements have skittered between public and private realms in recent years – from for-profit contractors employed by airports and paid for by airlines (prior to 9/11) to a federal agency partly funded by special taxes, with some recent moves toward a mixed system involving both public and private players.[2] The problem of determining who should do what, and what criteria should guide assignment becomes more complex and more consequential as the repertoire of delivery models expands.

Joint action for infrastructure protection is all but inevitable: Neither sector on its own likely possesses the requisite mix of information, resources, and incentives. And there is small hope that the nation will slide into the right arrangements along the path of least resistance.[3] For example, private owners of vulnerable assets, reasoning that war (including "war on terror") is government's concern, expect the public sector to do the heavy lifting. Government, in turn, sees firms' concentrated stakes in valuable assets as ample private incentive to invest in protection against low-probability but high-loss events. Efficient collaboration is not the natural outcome of incentives in alignment against well-posed threats, but a construct of analysis, transactional architecture, and management.

This chapter examines the application to infrastructure protection of a particular form of public–private collaboration that we term "collaborative governance." Drawing on our broader work on collaborative governance, we introduce policy challenges and responses that have been employed in other settings and that offer lessons for infrastructure protection. The policy record, with respect to low-probability, high-cost threats, provides many pitfalls to avoid and suggests few templates to apply. The ability of intricate networks to find fresh ways to fail tends to outpace society's ability to develop regulatory and other bulwarks against failure, as witnessed by power blackouts such as afflicted the northeastern United States in 2003. The government's stance on natural disasters is rarely prevention (the focus of this chapter), but rather mitigation of consequences. Here too, however, experience has shown the limitations of state and local regulations and response services, federal support, and private insurance markets. And the policy response to the grim possibilities illustrated by the 9/11 terrorist attacks is not fully formulated, let alone tested. Both success and failure, though, offer insight into how to align public and private interests and energies. Our intent in this chapter is not to definitively pinpoint the ideal configuration of collaborative arrangements for infrastructure security. Rather, we seek to array and illustrate the principles that guide wise choices in crafting and managing collaboration.

Elsewhere we have defined collaborative governance as "the pursuit of authoritatively chosen public goals by means that include engaging the efforts of, and sharing discretion with, producers outside of government."[4] Collaborative governance is distinguished both from simple contracting and from private voluntarism by the allocation of operational discretion. In a pure goods or services contract, the government retains all discretion – for example, New York City's government might hire a private firm to put up barricades along a Midtown parade route. Pure voluntary provision would be illustrated by the Midtown Manhattan Association hiring private guards to patrol a particular

stretch of the route. Volunteerism places all discretion with the donor. At these two extremes, strategic interaction is relatively sparse.

In collaborative governance, by contrast, each party helps to determine both the means by which a broadly defined goal is achieved and the specifics of the goal itself. A charter school, for example, receives public funds to educate the children in its charge. Within the broad parameters set by its charter, it has considerable flexibility with respect to curriculum, staffing, the length of the school day and year, and other key determinants of education. The shared discretion that is the hallmark of collaborative governance can augment the capacity available for public missions and increase the flexibility with which such missions are pursued. But a price is paid: Authority becomes ambiguous, strategic complexity grows, and agency problems proliferate.

Debates over physical security have long featured both a privileging of the state in principle, and a blend of public and private responsibilities in practice. Max Weber explicitly defined government as "the human community that successfully claims the monopoly of the legitimate use of physical force,"[5] and Hobbes reluctantly prescribed submission to Leviathan as the only remedy to the "war of all against all." Yet the U.S. Constitution – often considered the blueprint for the modern state – was written in the wake of a war fought in part by extra-governmental forces – Hessian mercenaries on the British side and the "Pennsylvania Associators" on the other.[6] More currently, the United States has relied on private forces in Iraq and elsewhere for functions that are only marginally distinguishable from classic combat operations.[7]

Although large-scale armed conflict tends to be the state's province today, private forces routinely engage in lower-level security functions. Most large universities, for example, have their own police forces to maintain order on campus and protect prominent or controversial guests who might excite violent protest. When public figures who are potential terrorism targets visit Harvard University, they are protected by a mix of public and private forces. A senior federal official might be guarded by the Secret Service and campus police while he gives his speech, with a phalanx of off-duty local police (paid by the university) monitoring entrances and exits and state police escorting him to and from the airport.

In short, long before terrorism became a major concern in the twenty-first century United States, collaborative approaches to protection – although not discussed in those terms – were both a subject of debate and a practical tool in the provision of security. To reap the benefits and curb the risks of collaborative arrangements for infrastructure security, one must understand the phenomenon more generally. For example, an appreciation of how we protect our food supply against contaminants or our hospital care against costly

error will help explain how to protect our ports and power plants against terrorism. Moreover, unless one can understand the forces that shape collaborative governance across a society, it is difficult to discern how best to allocate discretion and divide responsibility in the specific area of infrastructure protection.

This chapter begins with a few general observations on the rising – or to be more precise, restored – importance of non-governmental actors in public undertakings, a category that includes but goes beyond collaborative governance. Next, it probes some of the dynamics of shared discretion in the pursuit of public goals. Finally, it characterizes the fundamental challenge of a collaborative approach to infrastructure protection and the special imperatives the public sector must meet to perform its indispensable analytical and managerial functions within such arrangements.

Private engagement in governmental undertakings – both within and beyond the security arena – is neither new nor rare. Indeed, virtually every plausible blend of state and market organization has been observed in practice at some time and place. Nearly every developed nation's repertoire of collective-action models blends state and market components, but the preferred mix varies substantially by place, by time, and by project. Prominent private roles are the historical norm. But such roles seem novel against the backdrop of the extraordinary consolidation of federal authority in the mid-20th century. U.S. government spending exploded with the New Deal and World War II, from less than 4 percent of gross domestic product in 1930 to more than 44 percent 15 years later. Even after this wartime surge ebbed, federal spending rarely fell below 15 percent of gross domestic product, and the average for the second half of the twentieth century was 19.8 percent.[8] Quantitative expansion forced qualitative evolution as the mid-century heyday of the central government etched enduring patterns into organizational structures, administrative procedures, and the mindsets of scholars and practitioners.[9] Thus, we are apt to view delegated or shared public responsibilities as something novel. But constructing and maintaining arrangements for efficient and accountable public–private interaction has been, and is becoming once again, very much a mainstream task for managing the public's business.

RATIONALES AND RISKS OF INDIRECT GOVERNMENT ACTION

Non-governmental actors are appropriately enlisted into public undertakings – whether running a school or guarding a port – to improve performance in the creation of public value. Private entities may offer advantages over governmental organizations in several (partly overlapping) dimensions.

RESOURCES

Perhaps the simplest rationale for collaboration with the private sector arises when government lacks the resources (or the ability to mobilize the resources) required to accomplish a mission. Today, as empty public coffers coincide with urgent homeland security imperatives, this rationale holds special salience. In principle, "governmental resources" is both an imprecise and an elastic category. The U.S. government commands resources only as the citizens' steward, rather than on its own account. Its spending ability is not determined by its earning ability or its collateral available to support debt, but primarily by citizens' tolerance for taxation, including the future taxation implicit in public debt. So a declaration that government's resources are inadequate to realize some public goal translates to one or more possible scenarios:

- Citizens are unwilling to provide, through taxation, revenues to fund this particular undertaking – a situation that, if it strictly applied, should raise questions about whether the mission is accurately labeled as a "public goal."
- Citizens are not asked to provide designated resources for this particular goal, so one cannot assess their willingness to pay for it, but their tolerance of taxation in the aggregate is exhausted, or nearly so.
- Procedural impediments (budget rules, debt limits) preclude incremental funding for this goal independent of its merits, and resources cannot be or are not diverted from other purposes.
- Citizens are willing to devote resources to the mission, but not enough to accomplish it with public funds alone. Only if costs borne by government can be lowered through an infusion of non-governmental resources, or by improving operational efficiency through private involvement, will it meet the net benefits test from the public perspective.
- Some aspects of a public project provide benefits are so narrowly directed to particular groups – such as the owners of a chemical factory, nuclear facility, or port – that the electorate believes the prime beneficiaries should pay at least a share and are unwilling to fund the endeavor except on these terms.

PRODUCTIVITY

A second generic rationale for indirect government production is that external agents possess productive capacity and capability that government lacks. By collaborating with firms or non-profit organizations, the government can tap the outside entity's efficiency edge to improve performance or lower costs or both, relative to acting alone. In one variant of this rationale, technical know-how, proprietary intellectual capital, or other potentially transferable

capacity resides in the private sector instead of in the government. In a second variant, productivity advantages are not accidental but inherent in the private form of organization. Potential reasons for private advantages are familiar – the focused incentives of the profit motive (at for-profits) and procedural flexibility (at both for-profits and non-profits), the ability to harvest economies of scale and scope by operating beyond jurisdictional boundaries, and the motives inherent in the prospect that the quality of performance will affect the odds of extension, merger, or extinction. A third variant of the efficiency case for delegation has to do with standby capacity. If the need for a public undertaking arises only episodically – such as snow removal, disaster relief, or the Christmas-season surge in postal demand – it may be less costly to rely on the private sector for peak needs than for government to build up the surge capacity itself. (Or it may not; the choice turns on which sector, public or private, can better employ the standby resources when they are not needed to meet surge requirements.) The more important and embedded are private productivity advantages, the stronger the rationale for delegated, collaborative, or otherwise shared production.

INFORMATION

Even if the government's resources and productivity are identical to the private sector's, an initiative can be improved through private involvement when the government does not have pertinent information and would find it very difficult or prohibitively expensive to acquire it.[10] The types of data needed to carry out some publicly consequential task – such as information on the relative volatility and toxicity of different compounds in use at different locales within a chemical plant, or the docking schedule and processing time for various vessels and cargoes at a port – are often embodied in private organizations in ways that make it hard to share them with or sell them to government.

LEGITIMACY

Fans of old-time Westerns know that a group of citizens in hot pursuit of the bad guy was called a "posse" if the sheriff was involved and a "mob" if he was not. However, in some circumstances private involvement may enhance the perceived legitimacy of an undertaking. A particular task may be seen as inappropriate for the government to pursue on its own. Or if government is held in systematically low esteem by the citizenry, as in failed states or corrupt regimes, collaboration with the private sector can shore up legitimacy independent of any task-specific factors. In such circumstances, private-sector involvement may be necessary for effective public activity.

Legitimacy considerations may cut the other way, of course. Most people find it unremarkable for a private company to post night watchmen to guard against pilferage. But not many would endorse permitting the same company to send private interrogators to raid the homes of suspected pilferers; that is the government's job. When Ross Perot engaged private commandos to rescue two of his employees held hostage in an Iranian prison in 1979, some found it noble and some foolhardy, but few called for disbanding the U.S. State Department and the Special Forces in favor of Perot's self-service model. There may have been more of an outcry about private usurpation of a public responsibility if the employees had been imprisoned in Indiana rather than Iran.

GENERIC RATIONALES APPLIED TO INFRASTRUCTURE SECURITY

In many policy arenas, we have examined elsewhere – including park management, student loans, and foreign assistance – collaboration between the public and private sectors is an option that may or may not turn out to be superior to direct provision, regulation, simple contracting, or autonomous voluntarism.[11] In contrast, infrastructure protection by its very nature usually involves some degree of inter-organizational, cross-sectoral collaboration. In the United States, all chemical factories and airlines, most power utilities and electricity transmission assets, and many port operations and nuclear facilities are privately owned. Even when an airport or power plant is in the government's hands, it is usually far removed from the public entities responsible for security. Collaboration is thus a necessity, rather than an option – although the terms of that collaboration can vary over a wide range.[12] (In this chapter, we focus on the sharing of responsibility for terrorism loss *prevention*. Different considerations can apply to public–private collaboration for recovery from a terrorist attack.)

While a substantial private role in infrastructure protection may be all but inevitable, its extent and contours are open issues, and the generic rationales for private involvement – resources, productivity, information, and legitimacy – do come into play in the infrastructure arena, though often in distinctive ways. The change in airport security screening in late 2001, for example, illustrates a tendency to perceive the government as having an advantage in the security arena that departs from the general presumption of greater private-sector efficiency in delivery of services (see Box 24.1). On productivity grounds alone, a case could probably be made for government to handle most functions associated with infrastructure protection.[13]

BOX 24.1 AIRPORT SECURITY DOES AN ABOUT-FACE

The relative efficacy of public and private service provision was at the core of the debate over airport security that erupted immediately after 9/11. The existing system of private passenger screening was suddenly, and with near-unanimity, denounced as inadequate. A public mission newly perceived to be of paramount importance – ensuring that nobody bent on destruction could board an airliner armed – had been entrusted to a cheap, rickety delivery system. The airlines, many of them chronically on the verge of insolvency, had been required to pay for passenger screening, and they had bid out the work to a highly competitive industry of private security firms. But to eke out any profit from their lean contracts with the airlines, these security firms had drawn their workers from the bottom of the labor pool. Screeners' wages had been paltry and benefits generally negligible; standards, naturally, had been low and turnover high (for example, screener turnover at Chicago's O'Hare International airport had been more than 200 percent per year).

What was to replace this unacceptable status quo? One option was to move passenger screening alongside other crucial security functions carried out directly by the government. The other option was to continue to delegate screening to specialized private providers, but with more funding, far higher standards, and direct government oversight.

The Bush administration and its allies in the House of Representatives proposed an upgraded security system that would still rely on private providers. Rival Senate legislation crafted by Democratic leaders with the help of Republican maverick John McCain, called for making passenger and baggage screening a governmental function carried out by public employees. Many commentators predicted that President Bush would get his way, as he had with so much else in the wake of the terrorist attacks. But as the dust settled after a House–Senate conference on the airport security bill, the proponents of direct governmental delivery had won nearly every point. The final legislation called for virtually all passenger and baggage screening to be performed by federal employees under a new Transportation Security Authority. Applicants lined up for positions in the authority, and a year after the law was passed there were more than 60,000 federal passenger and baggage screeners on the job in America's airports. Their training was rigorous, their compensation far better than that of their private-sector predecessors, and their job satisfaction demonstrably higher; once hired as a government screener, few workers quit.

Security is very likely better than it was prior to 9/11 – although the overall rarity of hijacking makes it hard to measure – but it is less clear that the increment of increased safety is worth the sharp increase in costs, or that the Transportation Security Authority performs better than would have an upgraded private system. The gross flaws in the previous contractual model did not preclude structuring a sturdier contractual arrangement. The work, however vital, is readily specified: Inspect every passenger and every piece of luggage to ensure that no weapon can be smuggled onto an airplane. Evaluation is more straightforward for airport screening than for many other functions that are delegated contractually. The performance of individual screeners can be gauged through actions and devices, for example by constantly testing security with dummy weapons or bombs and levying painful financial penalties for any lapse. Several large firms already operate in the industry, and entry is relatively easy, making airport screening far more competitive than many other outsourced functions. Such arrangements are not merely hypothetical; they were and are the norm in Israel and in many European countries that are sadly familiar with terrorism.

It is almost unimaginable, however, that the private sector would be entirely absent from infrastructure security arrangements. Although a wholly private arrangement might not comport well with citizens' views of the private sector's proper role, a purely governmental arrangement could raise questions both about expansion of state authority and, on quite different grounds, about the propriety of sparing private organizations the potentially substantial costs of security for private assets.

The most consistently valid argument for a collaborative approach to infrastructure security turns on information. The government itself almost certainly lacks the fine-grained understanding of particular infrastructure assets (and their forward and backward economic linkages), necessary to mount the most robust and least costly defenses, and also to determine an appropriate level of effort. The private organizations that own, operate, or depend on physical assets would generally possess far more complete information of the sort relevant to the protection of those assets than would the government. Yet the public sector likewise can have privileged or exclusive access to information and procedural options – intelligence data, negotiations with foreign governments, the right to detain a suspect or tap a phone line – that could, in principle, be extended to the private sector but generally are not. The difficulty of efficient information sharing even between government agencies hints at the likelihood of even greater coordination hurdles for cross-sectoral security efforts. Indeed, serious legal barriers can prohibit or constrain private firms' efforts to share information with government.

COSTS AND RISKS OF PRIVATE ROLES IN PUBLIC MISSIONS

Indirect government action can expand the resources devoted to a mission, enhance the efficiency with which they are deployed, provide richer and more detailed information to guide the undertaking, or boost its perceived legitimacy.

Against these generic advantages, however, society must weigh a range of potential costs, which are commonly called "agency losses." That is, the private agents may not faithfully fulfill the public's mission; for example, they may purport to act at government's behest but instead give excess weight to parochial concerns. Direct government action often entails agency costs as well. Elected officials and government workers can and do pursue their own agendas at the expense of citizens' interests. Relationships that reach across sectoral boundaries summon four distinctive threats to effectively fulfilling public missions: diluted control, higher spending, reputational vulnerability, and diminished capacity.

Diluted control occurs as a result of indirect action that explicitly diminishes government's monopoly of authority for defining the mission, directing the means, or both. Beyond this open and accepted dilution of autonomy, indirect action also involves the risk of unanticipated or unrecognized losses of control.

Higher spending is also a potential threat. Indirect production can sometimes prove more costly than anticipated, and it can even be more expensive than direct production for the same output. This increased cost can be because of an erroneous prediction of private productivity advantages, because of transactions costs, because the dilution of control leads to a different and more costly definition of the mission, or because private actors are able to exploit and extract resources from their governmental partner.

Most forms of indirect action expose the government to some risk that the actions of its agents will adversely affect its reputation. For example, if the government requires (or merely allows) a nuclear plant operator to deploy a private security force, and if members of that force needlessly hinder innocent hikers in the surrounding woods, the citizenry's ire will fall on both public and private parties.

Diminished capacity can result when indirect production discourages or even precludes the maintenance of capacity for direct governmental action. To the extent government depends on private capabilities, it puts itself at a disadvantage in future rounds of negotiation with its agents. Whether such factors present trivial or profound barriers to reverting to direct governmental delivery, and whether reliance on external capacity entails minor or major future costs, will depend on the details of each case. If a village delegates trash collection to a private waste-management firm, it can later reconstruct the status quo by purchasing a truck and hiring two men; if a state privatizes its prison system, it would be far more costly to reverse course.

In complex, large-scale missions, including most instances of infrastructure security, neither a pure public nor a pure private solution is likely to be the best choice. The challenge is to develop a blend of public and private roles that amplifies the benefits and controls the risks presented by each sector. In this

light, it is useful to focus on the predominant feature that distinguishes collaborative governance from other forms of indirect governmental production – the explicit sharing of discretion.

SHARED DISCRETION AS THE HALLMARK OF COLLABORATIVE GOVERNANCE

Collaborative governance is defined by a mixed allocation of discretion. For an endeavor to be considered "governance" at all, a large share of discretion must rest with a player who is answerable to the public at large (where government is absent, weak, or undemocratic this condition is unlikely to hold). Collaboration begins when government yields the monopoly of control. Collaborative governance exists in the mid-range of the distribution of discretion; neither extreme can be considered collaboration. For example, corporate philanthropy is not collaboration. Companies enjoy wide discretion over their giving, and within very wide parameters their choices are presumptively defined as "the public good" for tax purposes. Although the public sector surrenders tax revenue it would have otherwise received, it is essentially a passive partner to the company's actions.

Similarly, a municipal government's contract with a private waste-management company is delegation but not collaboration. The company's mission to pick up the garbage and dump it at the landfill is explicit, complete, and controlled by the government, and its motive is to maximize the net revenue it receives in return. The private player is a highly constrained agent, nothing more, and discretion rests with the government. Understanding the ramifications of alternative allocations of discretion requires distinguishing among three forms of discretion: those involving production, payoffs, and preferences.

PRODUCTION DISCRETION

A fundamental motive for indirect governmental action is the realistic prospect of efficiency gains (relative to direct provision) through engaging private capacity. But this motive does not, on its own, call for collaborative governance. The government can often harness private efficiency advantages, while avoiding the complexities of shared discretion, through simple procurement contracts. If the government requires a truck, a bus route, or a software package, and recognizes that acquiring it from the private sector is likely to be more efficient than producing it internally, it can specify its requirements, invite competing bids, and choose the provider that promises to deliver on the best terms.[14] The contractor, once selected, is permitted a good deal of latitude over how

to go about meeting the terms of the deal, but the definition of ends remains government's prerogative.

In addition, in contracting for security services, it is often impractical, unwise, or flatly impossible for the government to fully specify its goals. For example, because the Department of Homeland Security has little understanding about what combination of ambulance drivers, nurses, and emergency room technicians would be most valuable to blunting a smallpox outbreak in Muncie, Indiana, it lets administrators at Ball Memorial Hospital set priorities for vaccinating "first responders." The Occupational Safety and Health Administration may focus on trash compactors as the greatest danger to grocery store employees, but the manager of the local Safeway may know that reducing loading-dock workers' risk of slipping on spilled produce would deliver far greater safety gains at the same cost. No government agency will likely match an automaker's judgment over the relative promise of innumerable changes in fuel, engines, design, and materials to boost mileage and hold down the costs of new-generation vehicles. And those who manage a liquefied natural gas (LNG) facility may know far better how to reduce its vulnerability to a terrorist attack than would government inspectors, both because of managers' familiarity with the operation of the facility and with other risks such as common crime, accidents, or disgruntled employees, all of which are somewhat analogous to, if less dire than, terrorism. Public goals often can be advanced more efficiently if private players are given some discretion not just over the means, but also over the ends to be pursued. When government yields a share of such discretion, it has crossed the line from simple delegation to collaborative governance.

In all but the most straightforward undertakings, permitting private agents to participate in the specification of what is to be produced, and how, greatly enhances the potential for efficiency improvements. Yet at the same time, the government may find it far more challenging to ensure accountability due to the two other forms of discretion that tend to be unwelcome concomitants of production discretion.

PAYOFF DISCRETION

Granting production discretion to private collaborators can increase the efficiency of governance and create more value than either direct government production or contractual delegation with tightly defined goals. However, the collaborating partners must deal with the distribution of that augmented pool of value. Allocating the payoff from any one productive arrangement can be conceptually rich and operationally complex, but matters become far more complicated when collaborations feature a choice among alternative arrangements that lead to different distributions of value. For example, an automaker

would favor a new-generation car campaign that relies heavily on reformulated fuel (imposing a fixed cost on the oil industry) rather than absorbing its own fixed cost of redesigned engines. If there must be new kinds of engines, however, the automaker would like to maximize the government's share of the research and development investment required. Similarly, a company that has already made progress on diesel-electric hybrids would like the campaign to anchor on that design rather than alternatives that play to the strengths of rivals. In short, once given discretion, private parties will attempt to shape the undertaking to increase their parochial payoffs.

When production alternatives entail different distributions of value, production discretion is inevitably entangled with payoff discretion. This makes the government vulnerable when it lacks full information about each alternative's efficiency and payoffs. When information is incomplete or private actors possess information that the government lacks, collaboration is apt to yield results that fall well short of what the potential could be if all information were fully shared. At worst, collaboration may lead to a choice of ends, and net gains in public value, that are inferior to what could be obtained through direct governmental production or through delegation by means of fully specified contracts. This risk is recognized, however, and explains why the government is normally chary about sharing discretion. On the other hand, conventional tactics for limiting the government's vulnerability to payoff discretion – such as tight performance goals, ceilings on agents' payoffs, or aggressive after-the-fact auditing – frequently sacrifice some of the efficiency gains of production discretion.

PREFERENCE DISCRETION

Payoff discretion has to do with the distribution value that can be expressed in monetary form. Preference discretion is a related but broader concept. Payoffs come in various forms that collaborators may value differentially. It is in the very nature of public missions that parties will differ in how they define the good. For example, a new private security arrangement in midtown Manhattan – say creating a protective cordon around a several-block area with random inspections of entering vehicles – may yield greater protection for buildings, but new inconveniences, reduced freedom of movement, and greater privacy invasion for the public. This arrangement may please the building owners who control the Midtown Manhattan Association, but displease pedestrians and hence the City Council.

As with payoff discretion, the challenge to efficient and accountable collaboration comes from the tendency for preference discretion to be entangled with production discretion. Government cannot be sure that a collaborator

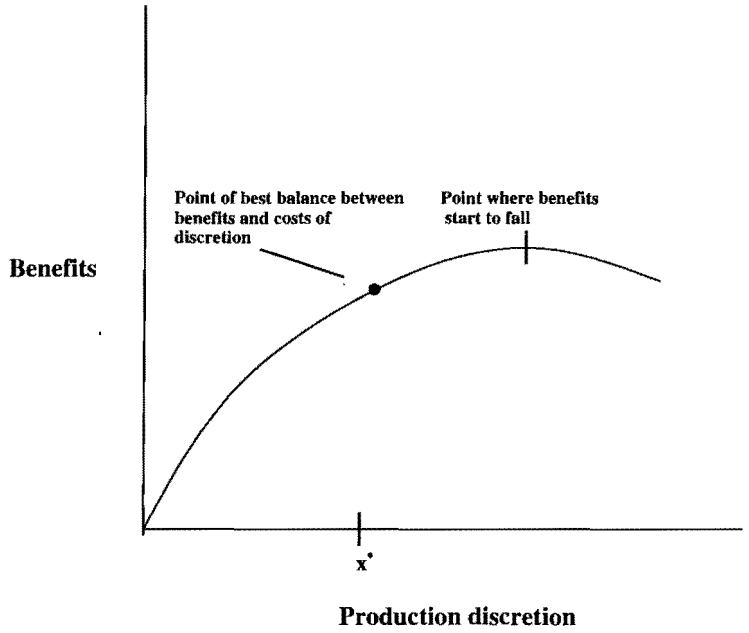

Figure 24.1. Production discretion boosts benefits (up to a Point).

is guided by his expertise or by his interests as he seeks to shape the mix of outputs the collaboration yields.

The central task for government officials attempting to create public value through collaborative arrangements is to maximize the efficiency gains of production discretion, after accounting for the losses associated with payoff and preference discretion. The optimal level of production discretion is found where the marginal benefit of production discretion equals the combined marginal costs of payoff discretion and preference discretion.[15]

The core task can be illustrated graphically, as well as stated in words and in equations. In Figure 24.1, the value gained through collaboration (relative to the polar cases of direct production or pure contracting) rises as private players are granted more production discretion. That discretion is exercised by choosing superior means for reaching a particular point, or by achieving production points unavailable to government acting on its own or through agents bound by tight contractual specifications. The gains of production discretion flatten as the potential of agents' productive and informational superiority is progressively exhausted. As discretion expands into areas where agents are less deft and worse informed than government – payoffs begin to diminish.

Alas, production discretion is generally accompanied by undesirable private discretion over payoffs and preferences. (To simplify the exposition, we

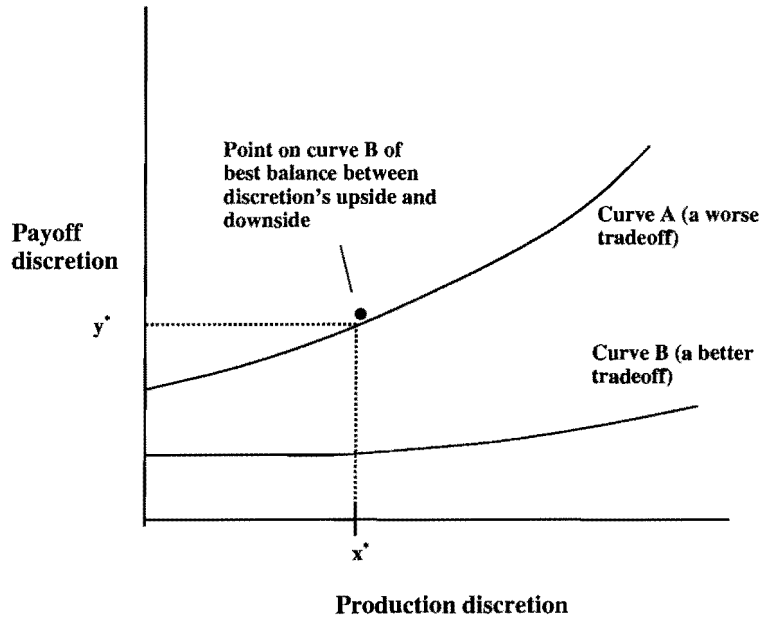

Figure 24.2. Payoff discretion as unwelcome fellow traveler of production discretion.

merely discuss payoff discretion here. The analysis for preference discretion would be much the same.) The ratio between production and payoff discretion is by no means a constant. Figure 24.2 shows two different trajectories of the relationship between these two types of discretion. Some payoff discretion is unavoidable, as shown by the vertical intercepts of the production possibility curves. Curve A illustrates a situation in which relatively little additional payoff discretion is incurred at the early stages of the range. The balance becomes somewhat worse as government continues to loosen constraints on private collaborators. Curve B illustrates a less-fortunate marginal relationship between production and payoff discretion.

Figure 24.2 might be thought of as illustrating two different arenas of collaborative governance, one with an inherently favorable relationship between good and bad discretion and the other with a more troublesome entanglement. Curve A might illustrate an "adopt a highway" program, in which local businesses take responsibility for clearing litter from a stretch of road in exchange for being allowed to post signs that publicize their civic-mindedness (as well as their donuts or health-care services through name recognition). Curve B might depict the hypothetical midtown-Manhattan security scenario addressed in the previous section, in which structures can be secured at a steep price in convenience and privacy. In the first case, the nature of the task itself presents private agents with limited opportunities to expropriate payoffs or insinuate

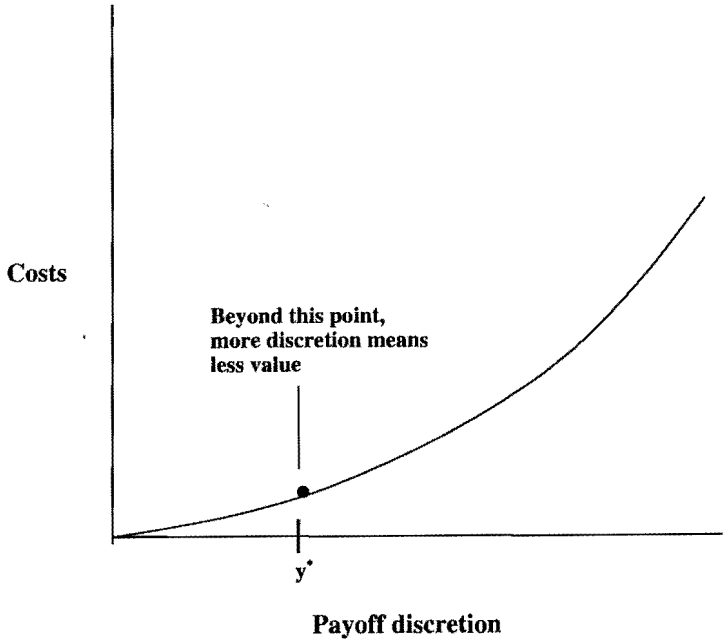

Figure 24.3. The degree of payoff discretion to accept.

preferences as they are given progressively more production discretion. In the second case, the temptation to push private interests, at the expense of the public interest, is pervasive.

Alternatively, and just as validly, Curves A and B can be thought of as referring to the same collaboration, but with more- and less-sophisticated governmental efforts to structure and manage the relationship. Curve B, in this version, would represent a feebly designed adopt-a-highway or city security program. Curve A would represent the same endeavor, but with more astute measures to harvest the gains while minimizing the losses that come with private discretion. In the highway case, for example, signs identifying benefactors might be smaller but more frequent to solidify the link between a company's image and the condition of a given stretch of roadway. In the security case, a Curve A scenario might involve the government requiring that arrangements be submitted to and approved by the City Council before being implemented, or it could institute a complaints process with stiff financial penalties levied against the private association in the event of unreasonable impositions on citizens.

While Figure 24.2 shows how payoff discretion rises with the level of production discretion, Figure 24.3 shows how much this costs. The value lost through payoff discretion grows as government loosens the reins, with the rate of loss

accelerating as government exercises less control over its collaborators' ability to claim larger payoffs or to substitute their preferences for those of the public at large.

For simplicity, we assume there is no preference discretion, or that it is costless. The optimum allocation of discretion is derived from the three functions represented on Figures 24.1, 24.2, and 24.3. It is found at x^*, implying that payoff discretion will be at y^*, and that the program will operate at the points along the curves corresponding to y^* (note that the marginal benefit of greater production discretion, the slope at the point of the curve corresponding to x^* in Figure 24.1, just equals the marginal cost). The latter is the product of the slopes at points B and C in Figures 24.2 and 24.3. That product represents the increase in payoff discretion from a unit increase in production discretion times the marginal cost of that increase. Parallel figures to 24.2 and 24.3 could be presented for preference discretion. They would have the same general shape. In weighing how much production discretion to grant, the counterbalancing costs of the accompanying payoff and preference discretion would be added together.

The outcomes for the public of collaborative governance, as these illustrations hint, can range from spectacular to calamitous, depending on government officials' ability to determine when collaboration is a promising approach, to judge how much discretion to cede to private agents, and to fine-tune the terms of the collaboration so as to maximize the benefits less the costs associated with shared discretion.

RISKS OF COLLABORATIVE APPROACHES TO INFRASTRUCTURE SECURITY

The risks of a collaborative approach to infrastructure security involve both payoff and preference discretion. The most obvious vulnerability associated with payoff discretion involves the allocation of costs. The managers of private firms involved in collaborative security efforts – assuming that they are faithful stewards for their shareholders – would prefer to maximize the government's share of the protection bill, including costs incurred for security benefits that fall to the firm itself rather than to the public at large. This logic extends to firms' natural desire to minimize any cost-increasing or profit-decreasing constraints on their operations. For example, imagine that building a triple-fence security perimeter patrolled by National Guardsmen could reduce by 90 percent the public risks of an attack on a chemical plant, at a discounted lifetime cost of $100 million. And suppose that reformulating the plant's product line or performing strict security vetting of all employees could achieve the same reduction for a mere $50 million. If the government pays most of the cost for

the first option and the firm pays all for the second, one would expect the private collaborator to use its discretion to tilt toward the perimeter patrol.

Similarly, firms will generally wield their discretion to favor anti-terrorism measures that offer ancillary private benefits. Installing floodlights throughout a port can deter petty theft and vandalism as well as terrorism, and a recent report from the Inspector General at the Department of Homeland Security suggests payoff discretion has been at work in the allocation of public port-security money. A port adjacent to a luxury entertainment complex (a target for security threats completely unrelated to terrorism) received a grant for surveillance equipment that the auditors found to "support the normal course of business" rather than respond to realistic terror threats.[16]

A systematic hazard involving payoff discretion is embodied (although experts differ as to what degree) in the Terrorism Risk Insurance Act of 2002 (TRIA), that introduced considerable public cost-sharing without curbing private discretion. This law was enacted in response to complaints that private terrorism coverage had become expensive and sometimes unavailable in the wake of the 9/11 attacks. There were respectable arguments for and against major government participation in the insurance market – arguments that continue today. TRIA ended up socializing the upper range of losses from terrorism damage to property (see Chapter 19 for a discussion of the components of TRIA). For risks covered by TRIA, private-property owners see little payoff in reducing their exposure to risks above the ceiling where government bears most of the cost, particularly because their insurance companies are unlikely to reward them for doing so. The distribution of losses from a terrorist act can be expected to dampen their incentive to invest in risk reduction, relative to alternative insurance arrangements, though the extent of the distortion is a matter of debate.[17]

Each firm in an industry would also like shared security regimes to be structured in ways that favor their business strategies over competitors'. A nuclear plant that has been operating for a long time, with 20 years' worth of spent fuel rods stored on the premises, will push for protection policies focused on nuclear waste; a newer plant will see more payoff in policies that concentrate on threats to the reactor itself. Requirements for a half-mile buffer zone around ports handling hazardous cargoes – accompanied by limited grants to buy adjacent land – would be devastating to a port in the middle of a dense, pricey city, but quite acceptable (and possibly even attractive for its competitive edge) for a port in an isolated community.[18]

Infrastructure security poses fewer obvious problems of conflicting preferences among collaborating parties than do some other arenas for public–private collaboration. Despite differing interests on the allocation of cost, and on the details of security arrangements, the basic goal of reducing expected terrorist losses is shared by government, private asset owners, and security owners. In social services, by contrast, some people consider it a very good thing if religious messages accompany substance-abuse counseling, and some people consider it a very bad thing. In matters of infrastructure protection, interests about salient choices are reasonably aligned. Everyone dislikes risk and would prefer to spend efficiently.

Yet even here there is room for divergent preferences at the margin, and private discretion can entail public costs. Private firms may also value the *perception* of security as well as its reality. Customers and possibly investors may find it hard to gauge levels of or changes in risk, and they may respond to visible risk-reduction measures as well as (or instead of) real but obscure reductions in the probability of a damaging attack. Private collaborators, moreover, will also prefer arrangements that give them privileged access to public security resources. To the extent that a major employer can shape the contingency plan for a regional alert, it would send more police and National Guardsmen to the local chemical plant than to the local hospital, school, or armory. Public and private players may also have different time preferences. A firm may doubt that investors will have much tolerance for short-term security spending in the name of long-term risk reduction. The government also has its own reasons for truncated time horizons, such as limited terms in office.

SECURITY EXTERNALITIES

In an alternative universe in which governments did not exist – but terrorism did – the private sector would assuredly take major steps to reduce the risk of attacks on infrastructure and to buffer the damage should an attack occur. Companies that own a particular asset would be motivated by the fact that terror attacks are bad for business. They destroy or damage capital assets, kill or injure employees with firm-specific skills, disrupt operations while facilities are repaired or rebuilt, suppress demand because customers are scared away, and raise the cost and reduce the availability of insurance against all these prospects. A rational company – with no motive other than maximizing the expected present value of net revenues – would spend on infrastructure protection up to the margin where its private value of incremental risk reduction reached its private cost of further security. Yet infrastructure protection is a governance challenge, not merely a business challenge, because threats to critical infrastructure have costs, and thus risk reduction has benefits, that extend far beyond private owners of infrastructure assets. Attacks on infrastructure can destroy neighboring assets. Collateral damage can be minor (the hot-dog stand adjacent to the oil pipeline pumping station) or major (the metropolis down-wind from

the nuclear power plant). Beyond the direct cost of physical losses would be the loss of business for other companies that depended upon destroyed or damaged infrastructure. On the special ledger of human casualties, losses external to the private firm come in two forms. First, dead or injured employees are much more than bundles of firm-specific skills. Second, in many imaginable incidents involving infrastructure, employees themselves would account for a minority of human casualties. More generally, a private company would have only minor motives—proportional to its share of the economy—to worry about the prospect of diffuse economic damage as confidence drops in the wake of an attack.

The term "positive security externality" describes a situation in which protection spending by one party benefits another. Such externalities may stem from many sources. One party's security efforts may prevent damage that would spill beyond bounds of ownership; or the spending party may control one element in a vital chain of products; or information may be gained from the efforts of each party that purchases security. Private arrangements would recognize and respond appropriately to some of these external risks, even in a world without government. For example, a factory that depended on a rail link or pipeline would rationally pay some or most of the security costs for that asset, even if it did not own it. A sufficiently sophisticated insurance industry would lead firms to internalize many external liability costs. Even a rudimentary tort system would stimulate A to enhance safety for B beyond its own pure self-interested level. Quite apart from traditional incentive structures for exchange, insurance, and liability, one could expect to see cost sharing to protect assets. For example, citizens of a nearby city, recognizing their vulnerability, would likely chip in to protect a nuclear plant. But transactions costs are likely to be significant, and complex negotiations may degenerate into stalemate. Alas, there are apt to be impediments to highly efficient security arrangements when the owner of the asset to be protected collects only a small fraction of the benefits.

However inventive private arrangements might be, when externalities abound society should still expect an inadequate supply of security absent government participation. When there are multiple parties sharing in a public good, voluntary provision falls far short, and the tort system tends to get short circuited. Beyond this, security investments shift probabilities rather than creating certainties; this makes it harder to estimate production relationships or tell what level of security is being provided. The resulting information asymmetries create barriers to effective contracting, since participants cannot tell what they are getting for their contributions.

ALLOCATING THE COSTS OF SECURITY

In a world of underprovision, government may step in to help reach the appropriate social level of spending. The government has three main tools for altering

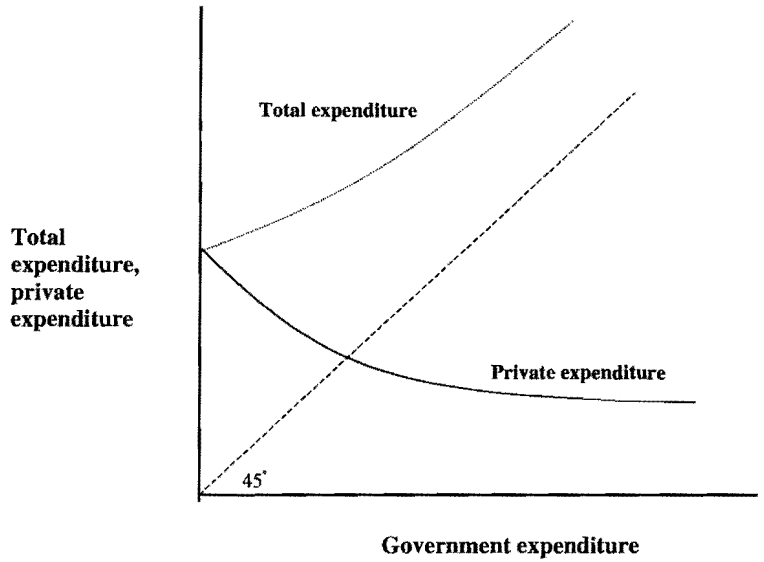

Figure 24.4. As government spends more, private spending sags and total spending lags.

private decisions about security: direct provision, regulation, and collaboration. Private companies, with plenty of alternative claims on their own resources, would naturally prefer for government to provide and pay for any needed security investments. But government budgets are chronically strained. Moreover, if they faithfully represent taxpayers' interests, governments will spend to reduce the public, but not the private, damages that a terror attack would produce. If security is left entirely to the public sector, then, there would be less spending on protection, in the aggregate, than the combination of public and private stakes would warrant.

A second objection to declaring security to be primarily or solely the government's burden is the question of equity. If the government is supposed to spend significant dollars protecting infrastructure, those who create infrastructure are in effect imposing a tax on the body politic. Moreover, infrastructure owners will have insufficient incentive to make their assets easy to protect. The situation might be as shown in Figure 24.4. Here the level of private provision and total provision is a function of the level of government provision. For simplicity, assuming that only total expenditure mattered, if private provision were strongly responsive to the level of public provision (i.e., the bottom curve slopes steeply), government provision would primarily shift costs to itself rather than enhance security.

When the government wishes to economize on public spending, but still achieve adequate security, it often adopts regulation. For example, insurance

companies must have adequate reserves, bicycle helmets must meet crash standards, and buildings must meet construction codes to protect against plumbing failures and fires. Some current regulations protect against terrorism. For example, nuclear power plants are required, as a condition of their licensing, to meet certain security standards. If the government knew precisely what should be done beyond these minimum standards, and if it had the power to impose desirable requirements, the regulatory approach would produce an ideal outcome for infrastructure security. But these are heroic "ifs." To some extent, these imposed expenditures offset other private expenditures. If the displacement is because those costs were inefficient, say because they tended merely to protect the spending party, then regulation can enhance efficiency. However, if the displaced costs would have created superior security, and the government regulation was chosen by mistake, say because of inadequate knowledge, or because certain expenditures are easier to monitor, then regulation will sacrifice efficiency.

In the collaborative governance approach, government extends certain benefits – such as cash or freedom from regulatory imposition, or the right to make claims on certain public resources – to private entities that agree to provide enhanced security. The advantages of collaboration are specific instances of the generic gains we discuss throughout this chapter. The deal the government strikes with the private players grants resources (which may include freedom from some governmental requirements) in exchange for the private sector taking on certain responsibilities. The private players may be protecting their own assets (e.g., the government could pay a third of the costs for a chemical company's security program); or they may be predominantly protecting other entities' private assets or even public assets (e.g., a port authority might hire a private firm to secure its facilities.) The nature, extent, and effect of private security efforts will be shaped by the government's stance, by the inherent interests of the private collaborators, and by the details of the collaboration's structure.

None of these three approaches to the problem of positive security externalities is likely to be fully successful, but some will be better than others at aligning resources with interests. When the externalities are small relative to the benefits going to the spending party, concerns should be minimal. When there is just one affected party, rather than many, efficient contracting on security levels will require only moderate transactional complexity. Time and money requirements for meetings, contracts, and lawyers will not be so burdensome as to deter rational security efforts. But when there are many parties with stakes in the same security arrangements; limited liability; and externalized losses that are large relative to internalized losses, security externalities are less tractable. Consider an LNG facility that is worth $20 million, owned by a company with

a market value of $100 million. A potential terrorist attack could trigger an explosion that would produce a total of $3 billion in damages, with most of the losses suffered by neighboring populations, businesses, and interconnected systems.[19] For $10 million, the LNG facility can reduce the lifetime chance of such an explosion from 1.1 percent to 0.1 percent. Society at large would benefit from such an expenditure, because in probabilistic terms it saves 1 percent × $3 billion, or $30 million. Yet the owners of the LNG facility will not make the expenditure if their own risk is limited to the $20 million value of the plant itself. Even if tort claims by damaged neighbors meant large and inescapable liability costs in the event of an attack, the firm itself would never be willing to spend more than the $100 million it would lose if it were sued into bankruptcy. It would not be hard to imagine circumstances where the optimal level of security spending, for society as a whole, exceeded the market value of the asset owner.

When significant security externalities exist, the only way to achieve adequate investments in security is to have all affected parties contribute.[20] Economics provides a classic resolution to this problem, which is called the Lindahl solution.[21] Assuming that there is a public good (in this case security) that will be enhanced through expenditures by a particular party, the Lindahl solution finds the percentage shares of the costs that will lead all parties to demand the same quantity. We can illustrate this with another simplified hypothetical situation, this one involving a chemical plant that processes hazardous chemicals located next to a factory that is not a terrorist target, and near to a built-up commercial and residential zone. Suppose there is one spending party (e.g., the owners of the chemical plant), one external party with major stakes (e.g., the owners of the factory next door), and many other affected parties (e.g., nearby businesses and residents), each with relatively small stakes. The government represents the interests of the parties with individually small stakes. The Lindahl solution divides expenditures in proportion to benefits at the margin for the optimal total expenditure. If, for example, the spending burden were divided with 70 percent borne by the chemical plant, 10 percent by the neighboring factory, and 20 percent by the government, all three parties would favor a total security expenditure of $2 million. The chemical plant would spend $2 million on security, and collect contributions of $200,000 from the neighboring factory and $400,000 from the government.[22]

This sketch departs from reality in its assumption that the probabilities of an attack and, even more challenging, that the magnitude of risk reduction from the security measures, are known with some precision. Low-level probabilities are inherently hard to estimate because they offer little experience to rely upon. Normal statistical methods cannot be employed. Indeed, the vast majority of the time, nothing happens. Given that outcome, it is almost impossible to

distinguish between situations where nothing would have happened absent the security measure and nothing happened because of the security measure. This estimation problem is redoubled because security measures affect the actions of the terrorists themselves. For example, if an intended target is protected, the terrorist can turn to a softer alternative target.[23] When an attack on a protected target is made, the security measure may prevent or ameliorate damage, and/or raise costs to the terrorists. Computing the benefits of security measures in such complex situations is extremely difficult.

Given that the public and private producers are sure to be tussling over costs, responsibilities, and credits, and that their interests diverge, each will have an incentive to provide its own estimates of the risks faced and the benefits (often probabilistic) that its own efforts provide. The challenges of probabilistic estimation – given the massive uncertainties here – exaggerate any natural tendencies to distort estimates to serve one's own purposes. These inherent uncertainties, and the likely disagreement on what expected benefits and costs would flow from potential actions, amplify the challenge of structuring a fair and feasible accommodation when security externalities are significant, as they usually are.

Moreover, while the balancing of burdens and benefits – and hence the management of payoff discretion – is challenging at any single point in time and in purely technical terms, it has important inter-temporal and political dynamics as well. Suppose government is able to structure an arrangement with a major port operator that features just the right blend of public and private expenditure and just the right pattern of risk-reduction investment at the start of the deal. The port operator is compensated just enough, and on just the right terms, to induce it to recognize the security externalities associated with its operations. Suppose, then, that many years pass without a major domestic terrorist attack. The port operator will be tempted – to the extent the terms of the deal and government's vigilance permit – to use its discretion to tilt security expenditures away from risk reduction and toward activities that boost profitability (e.g., installing attractive lighting in its tourist areas). To the extent this occurs, collaborative infrastructure protection is likely to be viewed as "corporate welfare," and to lose political legitimacy.

GOVERNMENT'S IMPERATIVES IN COLLABORATIVE INFRASTRUCTURE PROTECTION

Efforts to protect vital infrastructure in the coming decades will almost certainly involve extensive interaction between business and government, frequently featuring the shared discretion that is the hallmark of collaborative governance.

These arrangements could turn out to be flexible and effective, or rigid and lame. They may make a limited claim on resources and allocate costs in ways that are both fair and efficient, or they may entail bloated costs tilted toward the government in ways that undercuts private prudence and sap the public's willingness to pay for security. Which subsets of the many possible futures that turn out will depend on many factors, including revelations yet to come on the nature and extent of terrorism risks.

Thus, a pivotal determinant of whether infrastructure protection turns out to be efficient and robust, or expensive and flabby, will be government's ability to structure collaborative arrangements that give private players the proper incentives and focus public resources on broad public security. What does government need to get matters right in order to minimize the gap between the public and private benefits of investments in infrastructure security? The public-sector challenges in this arena are a particularly intense variant of the generic imperatives of collaborative governance. We array those imperatives as six distinguishable (though neither disjoint nor strictly sequential) steps:

1. *Appraisal.* Before designing a collaborative infrastructure security effort, government must first appraise the threat-reduction goal. It must map, as precisely as the data permit, both the public and the private risks embodied in the status quo – the nature and dimensions of the threat, the degree to which public and private vulnerabilities overlap or diverge, and the major uncertainties surrounding this appraisal. This first step, in short, involves figuring out what success looks like.
2. *Analysis.* Once the goal is tolerably well framed, the government needs to understand the capabilities and motivations of the players who may be engaged to help pursue it. The government must identify the array of private actors who are either inherently or potentially involved in security efforts; analyze the productive potential or resources they can bring to the enterprise; determine the preference and payoff motivations built into their economic structure and context; and identify the main points of congruence and conflict with broader public security goals. It must also predict how a particular configuration of security efforts is likely to influence external threats.
3. *Assignment.* Government officials, taking their cues from their appraisal of the mission and their analysis of private actors' abilities and intents, need to determine which security functions should be assigned to each party in the collaboration. These functions may be assigned across and within the public and private sectors, in accordance with the best fit between each function and the attributes of the various candidates to perform it. "Assignment" is only an approximate term for what is often a system of rules and incentives

meant to influence the probability that certain kinds of actors will take on certain kinds of tasks.

4. *Architecture.* Once the players are determined, their roles are specified through the development of accountability structures that are consistent with each actor's capabilities, incentives, and constraints, and that focus their energies on the common mission. This architecture can involve contractual relationships, financial incentives, regulation, tax preferences, public opinion, reputation, and other components in varying blends and degrees of complexity. The more that shared discretion – our hallmark of collaboration – figures in the relationship, the more subtle and more elaborate the architecture of accountability is likely to be.
5. *Assessment.* Even the most astute government official is unlikely to get the appraisal, analysis, assignment, and architecture exactly right, given the massive uncertainties involved. The government must assess the security collaboration as it matures – revising early appraisals of the threat to be confronted, revisiting first-round analyses of what private actors can do and what they want, rethinking the assignment of roles and the governance architecture that codifies responsibilities.
6. *Adjustment.* Because requirements change and analyses can be mistaken, the assessment stage may lead to significantly changed prescriptions. Thus, assignments and the architecture that coordinates them may have to be recalibrated. Adjustments will be undertaken as priorities change, new evidence comes to light, or experience reveals new problems or possibilities.

Each of these tasks is quite challenging on its own, and challenging along dimensions – differential treatment of outside parties, analytical and transactional precision, flexibility – that tend to be especially problematic for government. Taken together, they present a much more impressive set of requirements to master. This complexity is generally true of collaborative governance, and intensely so for collaboration on infrastructure protection. Appraising the array of risks in the status quo and analyzing the incentives of potential collaborative actors, for example, requires disentangling broadly shared vulnerabilities from firm-specific risks. It also demands a detailed appreciation of individual firms' competitive standing, with and without security investment, and with and without an actual attack. Measures of progress, essential to assessment and adjustment, are inherently uncertain absent an attack.

The public sector thus has a difficult role to plan in infrastructure protection – but an imperative role. If any of these tasks is ignored or badly carried out, a regime to promote infrastructure security that involves extensive private involvement and substantial private discretion will be less effective, more expensive, or both, than it would otherwise be. These governmental tasks are

of an entirely different nature from more familiar security regulations, such as writing blanket regulations for nuclear-plant containment vessels, or sending a company of National Guardsmen to patrol a port. They are subtle, complex, and fundamentally analytical. In infrastructure security, perhaps to an even greater extent than other policy domains, collaborative governance implies a role for government that is different from but no less vital than more familiar roles – and a role for which government is, for the most part, not yet well prepared.

NOTES

1. Bureau of Labor Statistics 2003.
2. The airline security issue is discussed at more length in Box 24.1.
3. The thoroughly inadequate and terribly coordinated policies in the few days surrounding Hurricane Katrina show the impossibility of developing effective collaborative arrangements predominantly on the fly. Hurricanes are different, to be sure, than terrorism threats, but in many ways simpler. For example, they give considerable advance warning.
4. Moran et al. 2006.
5. Gerth and Mills 1946.
6. The Pennsylvania Associators were a private force organized by Benjamin Franklin to substitute for the state militia that Quaker Pennsylvania balked at mustering under public authority. The associators figure in Fisher 2004. Their origins and organization are described on pages 26–28.
7. Singer 2002.
8. Office of Management and Budget 2004.
9. Even in the heyday of direct government delivery, important work was delegated to the private sector, including in ways that we would call collaborative. We are grateful to Lewis M. Branscomb for reminding us of the "cooperative agreements" that let federal officials enlist private collaborators on terms of shared investment and shared discretion.
10. Coglianese et al. 2004.
11. For collaboration in park management, see Donahue 2003, and Donahue and Rosegrant 2004. For student loans, see Lundberg 2005. For foreign assistance, see Lundberg 2004.
12. Sometimes the choice of public or private security arrangements is less consequential than it seems. Paul DiMaggio and Walter Powell argue that institutions performing similar tasks tend to conform to similar models of operation, whatever their formal structure. See DiMaggio and Powell 1983.
13. The public's attitudes toward the appropriate provision of security, however, may be strongly shaped by the most recent dramatic failure. Government efforts to deal with Hurricane Katrina, which bring to mind many comparisons with protection against terrorism, may have dampened enthusiasm with the government as the guarantor of security. Failed effectiveness in a dramatic event may promote a "throw the rascals out" attitude.
14. The basic terms of the choice between internal production and contracting-out are described in Donahue 1989, chapter 5.

15. More formally, let x indicate the level of production discretion, with $f(x)$ giving net production benefits (Figure 24.1). Let $g(x)$ be the level of payoff discretion (Figure 24.2), and let $c(g(x))$ be the cost of payoff discretion (Figure 24.3). Similarly, let $h(x)$ be the level of preference discretion, and let $d(h(x))$ be the cost of preference discretion. Our optimality condition is that $f' = c'g' + d'h'$.
16. Lipton 2005.
17. Kent Smetters of Pennsylvania's Wharton School has suggested that under TRIA, private owners of vulnerable assets will under-invest in security when much of the cost of a catastrophic incident falls to government. TRIA's origins, provisions, and incentive effects are discussed in Smetters 2004. The key terms are covered on pages 16–17. But other analysts, including one of the editors of this volume, view TRIA more favorably and predict much less distortion of private motives to minimize risk. See Kunreuther and Michel-Kerjan 2004.
18. This would be the case whether the urban port is owned by a private firm or by a public agency such as New York's Port Authority.
19. For purposes of this illustration, we are assuming, as seems reasonable, that the facility owner would not or could not be forced to fully compensate other parties for the avoidable damage they suffer due to the facility's failure to take security externalities into account.
20. Attempting to achieve the same outcome through regulation will not work. The regulated party, if forced to pay all of the costs, may just drop out of the market, which is likely to be inefficient if others benefit from having its services in the market.
21. The solution was first described in Lindahl 1919.
22. This example posited a private contribution from a second major private party, the neighboring factory. Often, free-riding tendencies would defeat such spending. The government would then be forced to be the sole supplement to spending by (in this instance) the chemical plant. The government could simply say that it will contribute 30 percent to anything the plant spends whether through direct dollars or a tax incentive.
23. Thus, the societal gain from the measure will only be the difference in the expected damages between the two targets, something that is virtually never computed.

REFERENCES (All Chapters)

Adamic, L. A. undated. Zipf, Power-laws, and Pareto – A Ranking Tutorial. http://www.hpl.hp.com/research/idl/papers/ranking/ranking.html (accessed June 27, 2006).

Adams, J. 2001. Virtual Defense. *Foreign Affairs* 80: 98–112.

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. 2000. Second Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, edited by James S. Gilmore et al. Washington, DC.

Albert, R., H. Jeong, and A. Barabasi. 2000. Attack and Error Tolerance of Complex Networks. *Nature* 406: 6794.

Aljazeera. 2004. Full transcript of bin Ladin's speech. November 1. http://english.aljazeera.net/NR/exeres/79C6AF22-98FB-4A1C-B21F-2BC36E87F61F.htm (accessed January 12, 2006).

American Academy of Actuaries. 2005. Statement by American Academy of Actuaries' TRIA Subgroup on Extending or Replacing the Terrorism Risk Insurance Act of 2002 (TRIA) December 1. http://www.actuary.org/pdf/casualty/tria_dec05.pdf (accessed February 25, 2006).

American Enterprise Institute (AEI). 2005. Should the Terrorism Risk Insurance Act of 2002 Be Extended? July 8. http://www.aei.org/events/eventID.1099,filter.all/event_detail.asp (accessed February 25, 2006).

Anonymous. 2003. Communication between a security executive who requested anonymity and the author, April 5.

AON. 2005. Property Terrorism Update: TRIA In The Balance. AON Risk Services October. http://www.aon.com/about/publications/pdf/issues/AonPropertyUpdate-TRIA,Oct2005.pdf (accessed February 25, 2006).

Apt, J., L. B. Lave, S. Talukdar, M. G. Morgan, and M. Ilic. 2004. Electrical Blackouts: A Systemic Problem. *Issues in Science and Technology* 20(4): 55–61.

Apt, Jay, Daniel Hoffman, Howard Kunreuther, and Erwann Michel-Kerjan. 2006. Insurance Industry and Global Warming. Philadelphia, PA: Wharton School, Center for Risk Management.

Associated Press. 2005a. Bush and Clinton, in Thailand, Start Tour of Tsunami Region. *New York Times*. February 20.

Associated Press. 2005b. London Bombings Trigger Surge in Inquiries. AP Online. August 16.

Associated Press. 2006. Report: Telecoms Helped NSA Wiretapping. February 6. http://www.msnbc.msn.com/id/11202938/ (accessed February 28, 2006).

Bak, Per. 1996. *How Nature Works: The Science of Self-Organized Criticality.* New York: Springer-Verlag Telos.

Barabasi A-L., S. V. Buldyrev, H. E. Stanley, and B. Suki. 1996. Avalanches in the Lung: A Statistical Mechanical Model. *Physical Review Letters* 76(12): 2192–2195.

Barabasi, A-L. 2003. *Linked.* New York: Penguin Books.

Bell, Coral M. 1978. Decision-making by governments in crisis situations. In *International Crises and Crisis Management. An East-West Symposium,* edited by D. Frei. New York: Praeger Publishers, 50–58.

Benfield Group Limited. 2005. *Outrageous Fortune: Reinsurance Market and Renewals Review.* January, 13–15.

Benjamin, Daniel, and Steven Simon. 2005. *The Next Attack: The Failure of the War on Terror and a Strategy for Getting it Right.* New York: NY Times Books.

Bennis, W., and B. Nanus. 1997. *Leaders: Strategies for Taking Charge.* New York: Harper & Row.

Bequai, A. 2002. White Collar Crime: A Handmaiden of International Tech Terrorism. *Computers & Security* 21(6): 514–519.

Bergen, Peter. 2002. Al Qaeda's New Tactics. *New York Times,* November 15, A31.

Berinato, S. 2002. The Truth about Cyberterrorism. *CIO Magazine,* March 15. http://www.cio.com/archive/031502/truth.html (accessed May 2, 2003).

Bernstein, Peter L. 1996. *Against the Gods. The Remarkable Story of Risk.* New York: John Wiley & Sons.

Berrick, Cathleen A., Director, Homeland Security and Justice Issues. 2006. Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program. Testimony before the Senate Committee on Commerce, Science, and Transportation. February 9. Government Accountability Office, GAO-06-374T, Washington, DC.

Best's Aggregates & Averages. 2005. AM Best, Olde Wyke, N.J. p. 98.

Biographies in Naval History. 2001. Admiral Hyman G. Rickover. http://www.history.navy.mil/bios/rickover.htm (accessed June 27, 2006).

Block, Robert. 2005. U.S. Finds Ally in Terrorism Fight in FedEx: Since September 11, Firms Cooperate More Often with Officials, Raising Privacy Concerns. *Wall Street Journal Europe.* May 30, A6.

Boardman, Michelle. 2004. *Known Unknowns: The Delusion of Terrorism Insurance.* George Mason University School of Law, Paper 244. http://law.bepress.com/cgi/viewcontent.cgi?article=1593&context=expresso (accessed February 25, 2006).

Bosk, C. L. 2003. *Forgive and Remember: Managing Medical Failure.* Chicago: University of Chicago Press.

Boulter, J. 1995. Tic-Tac-Toe. http://boulter.com/ttt/ (accessed June 27, 2006).

Bourrier, M. 1996. Organizing Maintenance Work at Two American Nuclear Power Plants. *Journal of Crisis and Contingency Management* 4(2): 104–112.

Brady, Matt. 2006. TRIA Coverage Light, Says Moody's, January 19. National Underwriter Inc.

Braga, G. A., R. Sanchis, T. A. Schieber. 2005. Critical Percolation on a Bethe Lattice Revisited. *SIAM Review* (47)2: 349–365.

Branscomb, Lewis M. 2004. Japanese–American Collaborative Efforts to Counter Terrorism. In *The Bridge: Linking Engineering and Society: National Academy of Engineering* 34(2): 11–16.

Branscomb, Lewis M. 2006. Sustainable Cities: Safety and Security. *Technology in Society* 20(1–2): 225–234.

Brown, J., D. Cummins, C. Lewis, and R. Wei. 2004. An Empirical Analysis of the Economic Impact of Federal Terrorism Reinsurance. *Journal of Monetary Economics* 51: 861–898.

Buchanan, M. 2001. *Ubiquity.* New York: Three Rivers Press.

Bureau of Labor Statistics. 2003. Occupational Employment and Wage Estimates, National NAICS 3-digit Industry Specific Estimates spreadsheet. Occupational Employment Statistics Program. http://www.bls.gov/oes/oes_dl.htm#2003_m (accessed July 2004).

Burns, R. E., J. Wilhelm, J. McGarvey, and T. Lehmann. 2003. Security-Related Cost Recovery in Utility Network Industries. White paper National Regulatory Research Institute, Columbus, OH. http://www.nrri.ohio-state.edu/dspace/bitstream/2068/366/1/05-03.pdf (accessed February 2, 2006).

Bush, George W. 2001. Executive Order 13231. Critical Infrastructure Protection in the Information Age. White House, Washington, DC.

Bush, George W. 2002. Protecting Critical Infrastructure and Key Assets. National Strategy for Homeland Security. White House, Washington, DC. July 16.

Bush, George W. 2003a. Critical Infrastructure Identification, Prioritization, and Protection. *Homeland Security Presidential Directive 7.* White House, Washington, DC. December 17.

Bush, George W. 2003b. *Homeland Security Presidential Directive 8.* White House, Washington, DC. December 17.

Bush, George W. 2003c. Protecting Key Assets. *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.* White House, Washington, DC. February 2003, p. 2.

Bush, George W. 2004. Press Conference of the President, April 13. http://www.whitehouse.gov/news/releases/2004/04/print/20040413-20.html (accessed February 25, 2006).

Carney, Bill. 2005. TRIA Sunset and it's Impact on Workers' Compensation. *IAIABC Journal.* Fall. 42(2): 167. http://www.iaiabc.org/publications/journal/2005/IAIABC%20Journal%20Fall%202005%20Vol%2042(2)%20cover.pdf (accessed March 4 2006).

Cauley, Leslie, and John Diamond. 2006. Telecoms Let NSA Spy on Calls. *USA Today,* February 5. http://www.usatoday.com/news/washington/2006-02-05-nsa-telecoms_x.htmm (accessed February 28, 2006).

CBS News. 2005. Airline Passenger Privacy Betrayed, CBS News. March 26. http://www.cbsnews.com/stories/2005/03/26/politics/main683296.shtml (accessed November 2005).

Chalk, Peter, Bruce Hoffman, Anna-Britt Kasupski, Robert T. Reville. 2005. *Trends in Terrorism.* June. RAND Corporation, Santa Monica, CA.

Chandler, Alfred. 1977. *The Visible Hand: The Managerial Revolution in American Business.* Cambridge, MA: Belknap Press.

Chertoff, Michael. 2005. Second Stage Review Remarks. Speech at the Ronald Reagan Building, U.S. Department of Homeland Security. July 13. Washington, D.C. http://www.dhs.gov/dhspublic/display?content=4597 (accessed February 28, 2006).

Chisholm, D. 1989. *Coordination without Hierarchy: Informal Structures in Multi-Organizational Systems.* Berkeley, CA: University of California Press.

Clarke, L. 1993. The Disqualification Heuristic: When Do Organizations Misperceive Risk? *Research in Social Problems and Public Policy* 5: 289–312.

Clarke, Richard (ed.). 2004. *Defeating the Jihadists: A Blueprint for Action.* New York: Century Foundation Task Force Report.

Clinton, William J. 1995. U.S. Policy on Counter Terrorism. Washington, DC: White House.

Clinton, William. 1996. Critical Infrastructure Protection. Washington, DC: White House.
Clinton, William. 1998. U.S. Policy on Counter Terrorism. Washington, DC: White House.
Clinton, William. 1999. National Infrastructure Assurance Council. Washington, DC.
CNN. 2002. Official: Voice on Tape is bin Laden's, November 13. http://archives.cnn.com/2002/WORLD/meast/11/12/binladen/statement/ (accessed January 12, 2006).
Coalition for Secure Ports. 2005. Fact sheet. http://www.secureports.org/improving_security/factsheet_screening.html (accessed November 2005).
Coalition to Insure Against Terrorism (CIAT). 2005. Fed Chairman Questions Ability of Private Market Alone To Insure against Terrorism. Press release, February 17. http://www.cmbs.org/Terrorism_Insurance_Files/2_17_05_CIAT_Press_Release.pdf (accessed February 25, 2006).
Coglianese, C., and D. Lazer. 2003. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals. *Law & Society Review* 37: 691–730.
Coglianese, Cary, Richard J. Zeckhauser, and Edward Parson. 2004. Seeking Truth for Power: Informational Strategy and Regulatory Policymaking. *Minnesota Law Review* 89(2): 277–341.
Collins, Susan. 2006. Luncheon speech, conference on Protecting Our Future, National Press Club, Washington DC, March 15.
Coluccio, F. 2005. Of Fiber Cuts and Mega RBOC Mergers. http://www.merit.edu/mail.archives/nanog/2005-08/msg00332.html (accessed March 14, 2006).
Columbia Encyclopedia. 2004. Rickover, Hyman George. http://www.bartleby.com/65/ri/Rickover.html.
Comfort, Louise. 2002a. Governance Under Fire: Organizational Fragility in Complex Systems. Paper presented at Symposium on Governance and Public Security, Syracuse, NY, January 18.
Comfort, Louise. 2002b. Institutional Re-orientation and Change: Security as a Learning Strategy. *The Forum* 1(2).
Commission of European Communities. 2005. Green Paper on a European Programme for Critical Infrastructure Protection. Brussels. November 17.
Commission on National Security. 2001. New World Coming: American Security in the 21st Century. Washington, DC.
Commission on the Intelligence Capabilities of the United States. 2005. Report Regarding Weapons of Mass Destruction. March 3. http://www.wmd.gov/report/report.html#chapter9 (accessed November 2005).
Commission on the Roles and Capabilities of the U.S. Intelligence Community. 1996. Preparing for the 21st Century: An Appraisal of U.S. Intelligence. http://www.gpoaccess.gov/int/report.html (accessed November 2005).
Con Edison. 2005. Con Edison Reports, earnings news release, http://www.coned.com/newsroom/news/pr20060126.asp?from=hc (accessed February 8, 2006).
Congressional Budget Office. 1983. Public Works Infrastructures: Policy Considerations of the 1980s. Washington, DC: U.S. Congress.
Congressional Budget Office. 2004. Homeland Security and the Private Sector. December. Washington, DC.
Congressional Budget Office. 2005. Federal Terrorism Reinsurance: An Update. January. Washington, DC.
Council on Competitiveness. 2002. Creating Opportunity Out of Adversity. Paper presented at National Symposium on Competitiveness and Security, December.

C-SPAN. 2005. Extending the Terrorism Risk Insurance Act of 2002. July 8.
Cukier, Kenneth Neil, Viktor Mayer-Schoenberger, and Lewis Branscomb. 2005. Ensuring (and Insuring?) Critical Information Infrastructure Protection. Working paper number RWP05-055. Cambridge, MA: Kennedy School of Government, Harvard University.
Cummins, D. 2005. Should the Government Provide Insurance for Catastrophes. Paper presented at the 30th Annual Economic Policy Conference, Federal Credit and Insurance Programs, Federal Reserve Bank of St. Louis, October 20–21.
Customs and Border Protection. 2004. Securing the Global Supply Chain: C-TPAT Strategic Plan. Washington, DC: U.S. Government Printing Office, November.
Dacy, Douglas C., and Howard Kunreuther. 1969. *The Economics of Natural Disasters: Implications for Federal Policy.* New York: The Free Press.
Daniels, R., D. Kellt, and H. Kunreuther (eds.). 2006. *On Risk and Disaster: Lessons from Hurricane Katrina.* Philadelphia: University of Pennsylvania Press.
de Bruijne, M., M. van Eeten, E. Roe, and P. Schulman. In press. On Assuring High Reliability of Service Provision in Critical Infrastructures. *International Journal of Critical Infrastructures.*
Dean, J. 2002. Report Stresses Management's Role in Boosting Cybersecurity. http://www.govexec.com/dailyfed/0202/021402j1.htm (accessed May 2, 2003).
Defense Threat Reduction Agency. 2003. Program Review. March 3. Arlington, VA.
Degnan, John. 2003. Statement of John Degnan to the National Commission on Terrorist Attacks Upon The United States. November 19. National Commission on Terrorist Attacks upon the United States. http://www.globalsecurity.org/security/library/congress/9-11_commission/031119-degnan.htm (accessed March 3, 2006).
Dempsey, James. 2004. Moving from "Need to Know" to "Need to Share": A Review of the 9/11 Commission's Recommendations. Testimony to the House Committee on Government Reform. http://www.markle.org/downloadable_assets/james_dempsey_testimony_080304.pdf (accessed November 2005).
Department of Energy. 1993. Earning Public Trust and Confidence: Requisite for Managing Radioactive Waste. Washington, DC: Task Force on Radioactive Waste Management, Secretary of Energy Advisory Board.
Department of Energy. 2003. Causes of the August 14 Blackout in the U.S. and Canada. Washington, D.C. U.S.–Canada Power System Outage Task Force.
Department of Homeland Security. 2004. Survey of the Information Analysis and Infrastructure Protection Directorate. February, OIG 04–13.
Department of Homeland Security. 2006. Personal communication by the NIPP office at DHS to the author, January 20.
Department of Justice. 2001. Press release. http://www.cybercrime.gov/ivanovIndict2.htm (accessed March 14, 2006).
Department of State. 2005. Country Reports on Terrorism. Office of the Coordinator on Counterterrorism. http://www.state.gov/s/ct/rls/45321.htm (accessed January 12, 2006).
Devol, R. C., A. Bedroussian, F. Fogelbach, N. H. Goetz, R. R. Gongalez, and P. Wong. 2002. The Impact of September 11 on U. S. Metropolitan Economies. Milken Institute, Santa Monica, CA. http://www.milkeninstitute.org/pdf/National_Metro_Impact_Report.pdf (accessed February 25, 2006).
DiMaggio, Paul J., and Walter W. Powell. 1983. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review* 48(2): 147–160.
Dixit, A. K. 2003. Clubs with Entrapment. *American Economic Review* 93(5): 1824–1829.

Dixon, Lloyd, and Rachel Kaganoff Stern. 2004. *Compensation for Losses from the 9/11 Attacks.* MG-264-ICJ. Santa Monica, CA: Rand Corporation.

Dixon, Lloyd, and Robert Reville. 2005. National Security and Compensation for Terrorism Losses. Catastrophic Risks and Insurance, Policy Issues in Insurance No. 8, Organization for Economic Co-operation and Development, 59–71.

Dixon, Lloyd, John Arlington, Stephen Carroll, Darius Lakdawalla, Robert Reville, and David Adamson. 2004. *Issues and Options for Government Intervention in the Market for Terrorism Insurance.* OP-135-ICJ. Santa Monica, CA: Rand Corporation.

Doherty, N. 2000. *Integrated Risk Management.* New York: McGraw-Hill.

Donahue, John D. 1989. *The Privatization Decision: Public Ends, Private Means.* New York: Basic Books.

Donahue, John D. 2003. Parks and Partnership in New York City A: Adrian Benepe's Challenge. Cambridge, MA: Kennedy School of Government Case Program.

Donahue, John D., and Susan Rosegrant. 2004. Parks and Partnership in New York City B: The Spectrum of Engagement. Cambridge, MA: Kennedy School of Government Case Program.

Donahue, John D., and Richard J. Zeckhauser: 2006. Public–Private Collaboration. In *The Oxford Handbook of Public Policy,* edited by Michael Moran, Martin Rein, and Robert E. Goodin. New York: Oxford University Press.

Economist. 2003. Fighting the worms of mass destruction. November 27. http://www.economist.co.uk/science/displayStory.cfm?story_id=2246018 (accessed May 2, 2003).

Economist. 2005a. Horrible Business: Terror Insurance. November 19.

Economist. 2005b. In Europe's Midst. July 16.

Electricity Consumers Resource Council (ELCON). 2004. The Economic Impacts of the August 2003 Blackout. Washington, DC: ELCON. http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf (accessed Feb 8, 2006).

Elias, Bart, W. Krouse, and E. Rappaprot. 2005. Homeland Security: Air Passenger Prescreening and Counterterrorism. RL32802, March 4. Washington, DC: Congressional Research Service.

Ellis III, J. Undated. Terrorism in the Homeland: A Brief Historical Survey of Violent Extremism in the United States. Memorial Institute for the Prevention of Terrorism, Oklahoma City.

Enders, W., and T. Sandler. 2000. Is Transnational Terrorism Becoming More Threatening? *Journal of Conflict Resolution* 44(3): 307–332.

Enders, W., and T. Sandler. 2006. *The Political Economy of Terrorism.* New York: Cambridge University Press.

Energy Advisory Board Task Force on Electric System Reliability. 1998. Final Report of the Secretary of Energy Advisory Board Task Force on Electric System Reliability, September 29. http://www.seab.energy.gov/publications/esrfinal.pdf (accessed February 2, 2006).

Energy Information Agency. 2003. Electricity Transmission Fact Sheet. Department of Energy, August 19. http://www.eia.doe.gov/cneaf/electricity/page/fact_sheets/transmission.html (accessed February 8, 2006).

Energy Information Agency. 2004. Electric Power Annual with data 2004, Table 2.2 Existing Capacity by Energy Source, 2004 (Megawatts). Department of Energy. http://www.eia.doe.gov/cneaf/electricity/epa/epat2p2.html (accessed February 8, 2006).

Etzioni, A. 1965. Organizational Control Structure. In *Handbook of Organizations,* edited by J. G. March. New York: Rand McNally.

Fairly, P. 2004. The Unruly Power Grid. *IEEE Spectrum* 41(8): 22–27.

Farrell, A. E., and H. Zerriffi. 2004. Electric Power: Critical Infrastructure Protection. In *Encyclopedia of Energy.* Amsterdam, Netherlands, Boston: Elsevier.

Farrell, A. E., H. Zerriffi, and H. Dowlatabadi. 2005. Energy Infrastructure and Security. In *Annual Review of Environment and Resources* 29: 421–469.

Farrell, A. E., L. B. Lave, and G. Morgan. 2002. Bolstering the Security of the Electric Power System. *Issues in Science and Technology* 18(3): 49–56.

Farrell, J., and G. Saloner. 1985. Standardization, Compatibility, and Innovation. *The Rand Journal of Economics.* Spring, 16(1): 70–83.

Farson, R., and R. Keyes. 2002. The Failure-Tolerant Leader. *Harvard Business Review* 64–71.

Federal Bureau of Investigation. 2001. E-commerce Vulnerabilities. NIPC Advisory 01-003, March 8. http://www.fbi.gov/pressrel/pressrel01/nipc030801.htm (accessed May 2, 2003).

Federal Bureau of Investigation. 2002. Terrorism 2000/2001. Publication 0328. Washington, DC: Department of Justice, Counterterrorism Division.

Federal Communications Commission. 2001. Network Outage Reporting System. http://ftp.fcc.gov/oet/outage (accessed May 7, 2003).

Federation of American Scientists. 2004. Tracing the Rise and Fall of Intelligence Spending: As Portrayed in Official Government Publications. June 7. http://www.fas.org/irp/budget/ (accessed November 2005).

Feinberg, Kenneth R. 2005. 9/11 Victim Compensation Fund: Successes, Failures, and Lessons for Tort Reform. January 13. Washington, DC: Comments at Manhattan Institute Center for Legal Policy Conference.

Feinberg, Kenneth R., Camille S. Biros, Jordana Harris Feldman, Deborah E. Greenspan, and Jacqueline E. Zins. 2004. Final Report of the Special Master for the September 11th Victim Compensation Fund of 2001. Washington, DC: U.S. Department of Justice. http://www.usdoj.gov/final_report.pdf (accessed January 9, 2006).

Fellman, P. V., and R. Wright. 2003. Modeling Terrorist Networks – Complex Systems at the Mid-Range. Conference on Complexity and Creativity, London School of Economics, UK, September. http://www.psych.lse.ac.uk/complexity/Conference/FellmanWright.pdf (accessed June 27, 2006).

Fellman, P. V., and R. Wright. Undated. Modeling Terrorist Networks – Complex Systems at the Mid-Range. http://www.psych.lse.ac.uk/complexity/Conference/FellmanWright.pdf (accessed March 22, 2006).

FERC. 2001. Statement of Policy on Extraordinary Expenditures Necessary to Safeguard National Energy Supplies. 96 FERC ¶61,299, Docket PL01-6-000. September 14.

Financial Services Sector Coordinating Council. 2005. Protecting the U.S. Critical Financial Infrastructure: An Agenda for 2005. http://www.fsscc.org/reports/FSSCC_2005_Agenda.pdf (accessed March 22, 2006).

Financial Times. 2005. Special Report on Business Continuity. June 27.

Finnegan, W. 2005. *The New Yorker,* July 25.

Finnegan, William. 2005. A Reporter at Large: The Terrorism Beat, *New Yorker.* July 25.

Fisher, David Hackett. 2004. *Washington's Crossing.* New York: Oxford University Press.

Florig, H. Keith. 2002. Is Safe Mail Worth the Price? *Science* 295: 1467–1468.

Flynn, M. F. 2005. Protective Security Division (PSD) Programs and Operations. Department of Homeland Security, March 8. http://www.nrc.gov/public-involve/conference-symposia/ric/past/2005/slides/03-b2-flynn.pdf (accessed March 7, 2006).

Flynn, Stephen E. 2004. The Neglected Home Front. *Foreign Affairs* 83(1): 20–33.

Flynn, Stephen. 2005a. Color Me Scared. *New York Times.* May 25.

Flynn, Stephen. 2005b. U.S. Senate Committee on Homeland Security and Government Affairs. The Security of America's Chemical Facilities: Testimony. 109: 1. April 27.

Fonow, R. C. 2003. Beyond the Mainland: Chinese Telecommunications Expansion. *Defense Horizons* 29: 1–8.

Frank, Thomas. 2004. Terror Warning Surprises Homeland Security Department. *Newsday*. May 28.

Frey, B. S. 2004. *Dealing with Terrorism: Stick or Carrot*. Cheltenham, UK: Edward Elgar Publishing.

Frey, Darcy. 1996. Something's Got to Give. *New York Times Magazine*. March 24, 42-ff.

Furnell, S. M., and M. J. Warren. 1999. Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium. *Computers & Security* 18(1): 28–34.

Gabrielov, A., V. Keilis-Borok, I. Zaliapin, and W. I. Newman. 2000. Critical Transitions in Colliding Cascades. *Physical Review E* (62) 1, 237–249.

Gerth, H. H., and C. Wright Mills (eds.). 1946. *From Max Weber*. Oxford, UK: Oxford University Press, 78.

Gertz, B. 2001. Al Qaeda Appears To Have Links with Russian Mafia. *Washington Times*. September 27.

Glasser, Susan B. 2005. U.S. Figures Show Sharp Global Rise in Terrorism State Department Will Not put Data in Report. *Washington Post*. April 27, A01.

Glassner, B. 1999. *The Culture of Fear: Why Americans Are Afraid of the Wrong Things*. New York: Basic Books.

Global Intelligence Challenges. 2005. Meeting Long-Term Challenges with a Long-Term Strategy, Testimony of Director of Central Intelligence Porter J. Goss Before the Senate Select Committee on Intelligence. http://www.cia.gov/cia/public_affairs/speeches/2004/Goss_testimony_02162005.html (accessed February 25, 2006).

Godard, Olivier, Claude Henry, Patrick Lagadec, and Erwann Michel-Kerjan. 2002. *Treatise on New Risks. Precaution, Crisis, and Insurance*. Paris: Gallimard, Folio-Actuel.

Goo, Sara Kehaulani. 2004. Confidential Passenger Data Used for Air Security Project. *Washington Post* January 17.

Gorman, Sean P. 2004. Networks, Complexity, and Security: The Role of Public Policy in Critical Infrastructure Protection. Ph.D. dissertation. School of Public Policy, George Mason University, Fairfax, VA.

Government Accountability Office (GAO; formerly General Accounting Office). 2002. Terrorism Insurance: Rising Uninsured Exposure to Attacks Heightens Potential Economic Vulnerabilities. Testimony of Richard J. Hillman before the Subcommittee on Oversight and Investigations, Committee on Financial Services, House of Representatives, February 27.

Government Accountability Office (GAO; formerly General Accounting Office). 2003a. Catastrophe Insurance Risks. Status of Efforts to Securitize Natural Catastrophe and Terrorism Risk. September 24, GAO-03-1033. Washington, DC: U.S. General Accounting Office. http://www.gao.gov/new.items/d031033.pdf (accessed February 25, 2006).

Government Accountability Office (GAO; formerly General Accounting Office). 2003b. Critical Infrastructure Protection: Efforts of the Financial Services Sector To Address Cyber Threats. Report to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Growth, Committee on Financial Services, House of Representatives Washington, DC: U.S. General Accounting Office. http://www.gao.gov/new.items/d03173.pdf (accessed May 7, 2003).

Government Accountability Office (GAO; formerly General Accounting Office). 2003c. Transportation Security: Federal Action Needed to Enhance Security Efforts. September 9, GAO-03-1154T. Washington, DC: U.S. General Accounting Office.

Government Accountability Office (GAO; formerly General Accounting Office). 2004a. Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors. April 21. GAO-04-699T. Washington, DC: U.S. General Accounting Office.

Government Accountability Office (GAO; formerly General Accounting Office). 2004b. Critical Infrastructure Protection: Improving Information Sharing With Infrastructure Sectors. GAO-04-780, July. Washington, DC: U.S. General Accounting Office.

Government Accountability Office (GAO; formerly General Accounting Office). 2004c. Determining Security Clearance Eligibility for Industry Personnel. May. GAO-04-632, Washington, DC.

Government Accountability Office (GAO; formerly General Accounting Office). 2004d. Security Clearances: FBI Has Enhanced its Process for State and Local Law Enforcement Officials. GAO-04-596, April. Washington, DC: U.S. General Accounting Office.

Government Accountability Office (GAO; formerly General Accounting Office). 2004e. Terrorism Insurance: Effects of the Terrorism Risk Insurance Act of 2002. May 18. GAO-04-806T, Washington, DC: U.S. General Accounting Office.

Government Accountability Office (GAO). 2005a. Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed. March. GAO-05-356. Washington, DC: U.S. General Accounting Office.

Government Accountability Office (GAO). 2005b. Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information During Secure Flight Program Testing in Initial Privacy Notices, But Has Recently Taken Steps to More Fully Inform the Public, Government Accountability Office, GAO-05-864R, July 22. Washington, DC: U.S. General Accounting Office.

Government Accountability Office (GAO). 2005c. Catastrophe Risk: U.S. and European Approached to Insure Natural Catastrophes and Terrorism Risks. February. GAO-05-199. Washington, DC: U.S. General Accounting Office. http://www.gao.gov/new.items/d03173.pdf (accessed March 3, 2006).

Government Accountability Office (GAO). 2005d. Protection of Chemical and Water Infrastructure: Federal Requirements, Actions at Selected Facilities, and Remaining Challenges. March, GAO-05-327. Washington, DC: U.S. General Accounting Office.

Grabowski, Martha, and Karlene Roberts. 1997. Risk Mitigation in Large-Scale Systems: Lessons from high Reliability Organizations. *California Management Review* 39(4): 152–162.

Grace, Martin, Robert Klein, Paul Kleindorfer, and Michael Murray. 2003. *Catastrophe Insurance*. Boston: Kluwer.

Graham, J. D., and J. B. Weiner (eds.). 1995. *Risk vs. Risk*. Cambridge, MA: Harvard University Press.

Green, J. 2002. The Myth of Cyberterrorism. November. *Washington Monthly*. http://www.washingtonmonthly.com/features/2001/0211.green.html (accessed May 2, 2003).

Green, R. M. 1980. Inter-Generational Distributive Justice and Environmental Responsibility. In *Responsibilities to Future Generations: Environmental Ethics*, edited by E. D. Partridge. Buffalo, NY: Prometheus Books.

Grid Today. 2003. Grid Technology Used to Hijack PC's? http://www.gridtoday.com/03/0721/101704.html (accessed May 2, 2003).

Grimmett, G. 1999. *Percolation.* Berlin, Germany: Springer-Verlag.

Guttman B., and K. Elburg. 2002. Israel: Cyber terrorism. *Computer und Recht International* 5: 156–157.

Halfele, W. 1990. Energy from Nuclear Power. *Scientific American* 263(3): 136–144.

Halsne, C. 2003. North Sound 911 Service Repeatedly Targeted. KIRO TV http://www.kirotv.com/news/2601577/detail.html (accessed May 7, 2003).

Hamilton, Donald. 2005. Telephone interview with Donald Hamilton, Executive Director, National Memorial Institute for the Prevention of Terrorism. Oklahoma City, OK. March.

Hardin, Garrett. 1968. The Tragedy of the Commons. *Science* 162(1968): 1243–1248.

Harrington, Caitlin. 2005. Former CIA Man Simmons Shoots Again for Unclassified Intelligence Unit at DHS. *CQ Homeland Security*, June 21.

Harris, Shane. 2004. Defense Department Lacks Staff to Tackle Security Clearance Backlog. GovExec.com. May 27. http://www.govexec.com/dailyfed/0504/052704h1.htm (accessed March 1, 2006).

Hartocollis, Anemona. 2005. Port Authority Found Negligent in 1993 Bombing. *New York Times*. October 27. http://select.nytimes.com/search/restricted/article?res=F30616F63A5B0C748EDDA90994DD404482 (accessed March 4, 2006).

Hartwig, Robert P. 2002. Industry Financial and Outlook – 2001 Year-End Results, Insurance Information Institute. http://www.iii.org/media/industry/financials/2001yearend/ (accessed June 23, 2004).

Hartwig, Robert. 2004. The Cost of Terrorism: How Much Can We Afford? National Association of Economics Conference. http://www.iii.org/media/presentations/tria/(accessed February 25, 2006).

Heal, G., and H. Kunreuther. 2005a. You Only Die Once: Interdependent Security in an Uncertain World. In *The Economic Impacts of Terrorist Attacks*,. edited by H. W. Richardson, P. Gordon and J. E. Moore II. Cheltenham, UK: Edward Elgar.

Heal, G., and H. Kunreuther. 2005b. IDS Models of Airline Security. *Journal of Conflict Resolution* 49: 201–217.

Heal, G., and H. Kunreuther. 2006. Security, Supermodularity and Tipping. NBER Working Paper 12281. June.

Heimann, C. F. L. 1993. Understanding the Challenger Disaster: Organizational Structure and the Design of Reliable Systems. *American Political Science Review* 87: 421–435.

Heinrich, C. 2005. *RFID and Beyond.* New York: John Wiley & Sons.

Heller, Miriam. 2001. Interdependencies in Civil Infrastructure Systems. *The Bridge* 31(4).

Hendershot, D. C. 2004. Inherently Safer Design, in *Accident Precursor Analysis and Management: Reducing Technological Risk Through Diligence*, edited by James R. Phimister, Vicki M. Bier, and Howard C. Kunreuther. Washington, DC: National Academy of Engineering, pp. 103–117.

Hendricks, K. B., and V. R. Singhal. 2005. An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price and Equity Risk of the Firm. *Production and Operations Management* 14(1).

Heymann, Philip, and Juliette Kayyem. 2005. *Protecting Liberty in an Age of Terror.* Cambridge, MA: The MIT Press.

Hobijn, Bart. 2002. What Will Homeland Security Cost? *Economic Policy Review* November, 21–33.

Hoekstra, Peter. 2005. Secrets and Leaks: The Costs and Consequences for National Security. July 29. WebMemo #809, Heritage Foundation. http://new.heritage.org/Research/HomelandDefense/wm809.cfm (accessed November 2005).

Hoffman, B. 1998. *Inside Terrorism.* New York: Columbia University Press.

Horch, Stephen, Howard Kunreuther, and Robert Gunter (eds.). 2001. *Wharton on Making Decisions.* New York: John Wiley & Sons.

Howarth, R. 1991. Inter-Generational Competitive Equilibria under Technological Uncertainty and an Exhaustible Resource Constraint. *Journal of Environmental Economics and Management* 21: 225–243.

http://www.psych.lse.ac.uk/complexity/Conference/FellmanWright.pdf (accessed June 27, 2006).

Hunter, J. Robert. 2004. The Terrorism Risk Insurance Act: Should it Be Renewed? April 19. Washington, DC: Consumer Federation of America. http://www.consumerfed.org/pdfs/terrorism_insurance_report.pdf (accessed February 25, 2006).

Iannaccone G., C. N. Chuah, S. Bhattacharyya, C. Diot. 2003. Feasibility of IP Restoration in a ier-1 backbone. Sprint Atlanta Technical Report TR03-ATL-030666, March. http://www.cambridge.intel-research.net/~gianluca/papers/restoration.pdf (accessed September 14, 2005).

Institute Of Medicine of the National Academies. 2005. Proceedings. Paper read at Protecting Against Foodborne Threats to Health. October 25–26.

Insurance Information Institute. Undated. Facts and Statistics. http://www.iii.org/media/facts/statsbyissue/catastrophes/ (accessed February 15, 2006).

Insurance Journal. 2005. Greenspan: Private Insurers Can't Cover Terror Risk Without Government. July 20. http://www.insurancejournal.com/news/national/2005/07/20/57478.htm (accessed February 25, 2006).

ISAC Council (Information Sharing and Analysis Centers Council). 2004a. A Functional Model for Critical Infrastructure Information Sharing and Analysis: Maturing and Expanding Efforts. ISAC Council white paper, January 31, 2004. http://www.isaccouncil.org/pub/Information_Sharing_and_Analysis_013104.pdf (accessed March 22, 2006).

ISAC Council (Information Sharing and Analysis Centers Council). 2004b. Government–Private Sector Relations. ISAC Council white paper, January 31, 2004. http://www.isaccouncil.org/pub/Government_Private_Sector_Relations_013104.pdf (accessed March 22, 2006).

ISAC Council (Information Sharing and Analysis Centers Council). 2004c. A Policy Framework for the ISAC Community. ISAC Council white paper, January 31. http://www.isaccouncil.org/pub/Policy_Framework_for_ISAC_Community_013104.pdf (accessed March 22, 2006).

Jaffee, D. 2005. The Role of Government in the Coverage of Terrorism Risks. Chapter 7 in *Terrorism Risk Insurance in OECD Countries.* Paris: OECD.

Jaffee, D., and T. Russell. 2005. Should Governments Support the Private Terrorism Insurance Market? WRIEC Conference, Salt Lake City, August.

Johnston, Donald. 2005. Dealing with Disasters and Protecting Critical Services: An International Perspective from the Organization for Economic Cooperation and Development (OECD). Address to the International Risk Governance Council 2005 General Conference, Beijing, September 20–21.

Jones, Donald, and Ronald Skelton. 1999. The Next Generation Threat to Grid Reliability–Data Security. *IEEE Spectrum* June: 46–49.

Kahneman, D., and A. Tversky. 2000. *Choices, Values and Frames.* New York: Cambridge University Press.

Kane, M. 2002. U.S. Vulnerable to Data Sneak Attack. CNET News.com. August 13. http://news.com.com/2100-1017-949605.html (accessed May 2, 2003).

Kauffman, Stuart. 1993. *The Origins of Self-Organization Selection in Evolution.* New York: Oxford University Press.

Kearns, M. 2005. Economics, Computer Science, and Policy. *Issues in Science and Technology* Winter: 37–47.

Kearns, M., and L. Ortiz. 2004. Algorithms for Interdependent Security Games. In *Advances in Neural Information Processing* Systems 16, edited by S. Thrun, L. Saul, and B. Scholkopf. Cambridge, MA: MIT Press.

Keohane, N., and R. Zeckhauser. 2003. The Ecology of Terror Defense. *Journal of Risk and Uncertainty*, Special Issue on Terrorist Risks, 26(2/3, March/May): 201–229.

Kettl, Donald (ed.). 2004. *The Department of Homeland Security's First Year: A Report Card.* New York: Century Foundation.

King, D., and M. G. Morgan. 2003. Guidance for Drafting State Legislation to Facilitate the Growth of Independent Electric Power Micro-Grids. Carnegie Mellon Electricity Industry Center Working Paper CEIC-03-17. http://wpweb2k.gsia.cmu.edu/ceic/papers/ceic-03-17.asp (accessed February 2, 2006).

Kleindorfer, P. R., and G. H. Saad. 2005. Managing Disruption Risks in Supply Chains. *Production and Operations Management* 14(1).

Kleindorfer, P. R., and L. Van Wassenhove. 2004. Risk Management for Global Supply Chains: An Overview. In *The Alliance on Globalizing*, edited by H. Gatignon and J. Kimberly. Cambridge, UK: Cambridge University Press.

Knake, Robert. 2005. Kennedy School of Government, interview with DHS PCII office, April.

Korten, D. 1980. Community Organization and Rural Development: A Learning Process Approach. *Public Administration Review* 40(5).

Kunreuther, H. 2001. Protective Decisions: Fear or Prudence. In *Wharton on Making Decisions*, edited by S. Hoch and H. Kunreuther. New York: Wiley.

Kunreuther, H. 2002. The Role of Insurance in Managing Extreme Events: Implications for Terrorism Coverage. *Risk Analysis* 22: 427–437.

Kunreuther, Howard. 2006. Has the Time Come for Comprehensive Natural Disaster Insurance? In *On Risk and Disaster Lessons from Hurricane Katrina*, edited by Ronald Daniels, Donald Kettl, and Howard Kunreuther. Philadelphia, PA: University of Pennsylvania Press, 175–202.

Kunreuther, Howard, and Geoffrey Heal. 2003. Interdependent Security. *Journal of Risk and Uncertainty* Special Issue on Terrorist Risk, March/May, 26: 231–249.

Kunreuther, H., and E. Michel-Kerjan. 2004. Challenges for Terrorism Risk Insurance in the United States. *Journal of Economic Perspectives* Fall, 18(4): 201–214.

Kunreuther, H., and E. Michel-Kerjan. 2005a. Insurability of (Mega)-Terrorism, Report for the OECD Task Force on Terrorism Insurance. In *Terrorism Insurance in OECD Countries*, Paris: Organization for Economic Cooperation and Development, July 5.

Kunreuther, H., and Michel-Kerjan, E. 2005b. Terrorism Insurance 2005. Where Do We Go from Here? Regulation. *The Cato Review for Business and Government*, Washington, DC: Cato Institute, Spring, 44–51.

Kunreuther, Howard, and Adam Rose (eds.). 2004. *The Economics of Natural Hazards*, two volumes. International Library of Critical Writings in Economics Series #178. Northampton, MA: Edward Elgar Publishing, Inc.

Kunreuther, Howard, et al. 1978. *Disaster Insurance Protections: Public Policy Lessons.* New York: John Wiley and Sons.

Kunreuther, H., P. McNulty, and Y. Kang. 2002a. Improving Environmental Safety Through Third Party Inspection. *Risk Analysis.* 22: 309–318.

Kunreuther, Howard, Geoffrey Heal, and Peter Orszag. 2002b. Interdependent Security: Implications for Homeland Security Policy and Other Areas. Policy Brief #108, October. Washington, DC: Brookings Institution.

Kunreuther, Howard, Erwann Michel-Kerjan, and Beverly Porter. 2003. Assessing, Managing and Financing Extreme Events: Dealing with Terrorism. November 20. Wharton School and National Bureau of Economic Research. http://opim.wharton.upenn.edu/risk/downloads/03-12.pdf (accessed February 25, 2006).

Kunreuther, Howard, Erwann Michel-Kerjan, and Beverly Porter. 2005. Extending Catastrophe Modeling to Terrorism. In *Catastrophe Modeling: A New Approach to Managing Risk*, edited by Grossi and Kunreuther, with Patel. New York: Springer.

Lagadec, Patrick. 1993. *Preventing Chaos in Crisis.* London: McGraw Hill.

Lagadec, Patrick, and Erwann Michel-Kerjan. 2005. A New Era Calls for a New Model. *International Herald Tribune*, Opinion, November 2.

Lagadec, Patrick, and Uriel Rosenthal (eds.). 2003. Anthrax and Beyond: New Challenges, New Responsibilities. *Journal of Contingencies and Crisis Management* Special Issue 11(3).

Lakdawalla, Darius, and George Zanjani. 2005. Insurance, Self-Protection, and the Economics of Terrorism. *Journal of Public Economics* 89: 1891–1905.

Landau, M. 1969. Redundancy, Rationality, and the Problem of Duplication and Overlap. *Public Administration Review* 27: 346–358.

La Porte, T. 1996. High Reliability Organizations: Unlikely, Demanding, and at Risk. *Journal of Contingencies and Crisis Management* 40: 60–71.

La Porte, T. R. 2003. Institutional Challenges for High-Reliability Systems Across Many Operational Generations – Can Watchfulness be Sustained? Paper presented at AAAS Symposium, Nuclear Waste: File and Forget? February 18, Denver, CO.

La Porte, Todd R. 2004. Challenges of Assuring High Reliability When Facing Suicidal Terrorism. Paper presented at workshop Private Efficiency, Public Vulnerability: Protecting Critical Infrastructure, Cambridge, MA, May 26–28.

La Porte, T. R., and P. M. Consolini. 1991. Working in Practice but Not in Theory: Theoretical Challenges of "High Reliability Organizations." *Journal of Public Administration Research and Theory: J-PART* 1(1): 19–48.

La Porte, T. R., and A. Keller. 1996. Assuring Institutional Constancy: Requisite for Managing Long-Lived Hazards. *Public Administration Review* 56(6): 535–544.

La Porte, T. R., and C. Thomas. 1994. Regulatory Compliance and the Ethos of Quality Enhancement: Surprises in Nuclear Power Plant Operations. *Journal of Public Administration Research and Theory* 5(4): 250–295.

LaPorte, T. R., K. Roberts, and G. I. Rochlin. 1989. High Reliability Organizations: The Research Challenge. Institute of Governmental Studies, University of California, Berkeley, April.

Lawyer, G. 2003. The Battle of the Bug: Government, Industry Move To Protect Internet from Cyber Attacks, Viruses. http://www.xchangemag.com/articles/1B1front4.html (accessed May 2, 2003).

Leavitt, Leonard. 2005. NYPD's Voice Loud and Clear. *Newsday.* October 14. http://www.nynewsday.com/news/local/newyork/ny-nyplaz144468713oct14,0,5267183.column?coll=ny-ny-columnists (accessed November 2005).

Lerner, A. W. 1986. There Is More than One Way to be Redundant: A Comparison of Alternatives for the Design and Use of Redundancy in Organizations. *Administration and Society* 18: 334–359.

Lerten, B. 2003. Tower Saboteur: I Was Only Pointing Out Flaws. *Bend Bugle*. November 23. http://bend.com/news/ar_view^3Far_id^3D12260.htm (accessed May 7, 2003).

Liang Q, Xiangsui. 1999. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House.

Lindahl, Erik. 1919. Die Gerechtigkeit der Besteuerung Lund: Gleerupska Universitets-Bokhandeln.

Lindstrom, A. 2001. Tunnel Vision? Broadbandweek.com. http://www.broadbandweek.com/news/010806/010806_news_fiber.htm (accessed July 23, 2002).

Lipson, H. F., and D. A. Fisher. 1999. Survivability – A New Technical and Business Perspective on Security. Proceedings of the 1999 New Security Paradigms Workshop, Caledon Hills, Ontario, Association for Computing Machinery.

Lipton, E. and K. Johnson. 2001. Tracking Bioterrorism's Tangled Course. *New York Times Magazine*. December 26, A1.

Lipton, Eric. 2005. Audit Faults U.S. for Its Spending on Port Defense. *New York Times*. February 20, A1.

Lipton, Eric. 2006. Chertoff Seeks a Chemical Security Law, Within Limits. *New York Times*, March 22. http://www.nytimes.com/2006/03/22/politics/22chemical.html (accessed March 27, 2006).

Little, Richard. 2002. Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures. *Journal of Urban Technology* 9(1): 109–123.

Loch, Stephen, and Howard Kunreuther (eds.). 2001. *Wharton on Making Decisions*. New York: John Wiley & Sons.

Lopez, Brian. 2003a. Critical Assets Workshop Guide: Lawrence Livermore National Laboratory, Vulnerability and Risk Assessment Program.

Lopez, Brian. 2003b. New Approaches Guidance: Lawrence Livermore National Laboratory, Vulnerability and Risk Assessment Program.

Lopez, Brian. 2004. Five Key Pieces on the Board: Lawrence Livermore National Laboratory, Vulnerability and Risk Assessment.

Lundberg, Kristen. 2004. Smarter Foreign Aid? USAID's Global Development Alliance Initiative. Cambridge, MA: Kennedy School of Government Case Program.

Lundberg, Kristen. 2005. Public Service or Gravy Train: The Federal Guaranteed Student Loan Program. Cambridge, MA: Kennedy School of Government Case Program.

Lunev, S. 2001. 'Red Mafia' Operating in the U.S. – Helping Terrorists. http://www.newsmax.com/archives/articles/2001/9/28/90942.shtml (accessed May 2, 2003).

Madigan, Sean. 2005. Shut Out: Overdue Security Clearances Make Fire Officials Smolder. May 2. *CQ Homeland Security*, Congressional Quarterly.

Maine PUC (Public Utility Commission). 2003. Docket Number 2002243. http://www.state.me.us/mpuc/misctranscripts/2002-243%20080503.htm (accessed May 7, 2003).

Mandelbrot, B. B. 1982. *The Fractal Geometry of Nature*. New York: W.H. Freeman and Company.

Marks, Alexandra. 2004. ABCs of the CIA: A To-Do List for Porter Goss. *Christian Science Monitor*. August 13.

Marsh Inc. 2005a. *The Impact of Nature: The Aftermath of Hurricanes Katrina and Rita*. November. http://solutions.marsh.com/hurricane/documents/MarshTheImpactofNature.pdf (accessed March 22, 2006).

Marsh Inc. 2005b. Marketwatch: Terrorism Insurance 2005. Research report. Marsh Inc. Item # 100162 04/05 Compliance # MA5-10185. http://www.marsh.dk/files/Marketwatch_Terrorism_Insurance_2005.pdf (accessed February 25, 2006).

Marsh, R. T. 1997. Critical Foundations. Washington, DC: Commission on Critical Infrastructure.

Mayntz, Renate, and Thomas P. Hughes (eds.). 1988. *Development of Large Technical Systems*. Berlin, Germany: Springer-Verlag.

McCall, William. 2005. City Council Approves Portland's Withdrawal from the JTTF. Associated Press from KATU News. April 28. Portland, Oregon.

McCullagh, Declan, and Anne Broache. 2006. Some Companies Helped the NSA, But Which? February 6. CNET News.com. http://news.com.com/Some+companies+helped+the+NSA,+but+who/2100-1028_3-6035305.html (accessed February 28, 2006).

McDonald, H. 2003. Beijing Spies a Useful Friend in Castro. *The Age*. February 27. http://www.theage.com.au/articles/2003/02/26/1046064102910.html (accessed May 2, 2003).

McWilliams, B. 2003. Cloaking Device Made for Spammers. http://www.wired.com/news/infostructure/0,1377,60747,00.html (accessed May 2, 2003).

Mendeloff, J. 1988. *The Dilemma of Toxic Substance Regulation: How Overregulation Leads to Underregulation*. Cambridge, MA: MIT Press.

Messmer, L. 2003. Navy Marine Corps Intranet hit by Welchia Worm. *Network World Fusion*. http://www.nwfusion.com/news/2003/0819navy.html (accessed November 10, 2003).

Michael, D. 1973. *On Learning to Plan and Planning to Learn*. San Francisco, CA: Jossey-Bass.

Michel-Kerjan, Erwann. 2003a. Large-scale Terrorism: Risk Sharing and Public Policy. *Revue d'Economie Politique* 113(5): 625–648.

Michel-Kerjan, Erwann. 2003b. New Challenges in Critical Infrastructures: A U.S. Perspective. *Journal of Contingencies and Crisis Management* 11(3): 132–141.

Michel-Kerjan, E. 2006. An Unnoticed Paradox: Insurance, the 14th Critical Sector. Working Paper, Center for Risk Management and Decision Processes. Philadelphia, PA: Wharton School.

Michel-Kerjan, E., and B. Pedell. 2005. Terrorism Risk Coverage in the Post- 9/11 Era: A Comparison of New Public–Private Partnerships in France, Germany and the U.S. *The Geneva Papers on Risk and Insurance*, 30(1): 144–170.

Michel-Kerjan, Erwann, and Nathalie de Marcellis-Warin. 2006. Public-Private Programs for Covering Extreme Events: The Impact of Information Sharing on Risk Sharing. *Asia-Pacific Journal of Risk and Insurance* 1(2): 21–49.

Mintz, John, and Susan Schmidt. 2004. Ashcroft Assailed on Terror Warning. *Washington Post*. May 28, A04. http://www.washingtonpost.com/wp-dyn/articles/A61742-2004May27.html (accessed November 2005).

Mintzberg, H. 1979. *The Structuring of Organizations*. Saddle River, NJ: Prentice-Hall.

Moran, Michael, Martin Rein, and Robert E. Goodin (eds.). 2006. *The Oxford Handbook of Public Policy*. New York and Oxford: Oxford University Press.

Morgan, M. G., and H. Zerriffi. 2002. The Regulatory Environment for Small Independent Micro-Grid Companies. *The Electricity Journal* 15(9): 52–57.

Morgan, M. Granger, Baruch Fischhoff, Ann Bostrom, and Cynthia J. Atman. 2002. *Risk Communication: A Mental Models Approach*. Cambridge, UK: Cambridge University Press.

Moteff, John D. 2000. Critical Infrastructures: Background and Early Implementation of PDD-63. Congressional Research Service, Report #RL30153. http://www.ncseonline.org/NLE/CRSreports/Science/st-46.cfm?&CFID=558905&CFTOKEN=30895709 (accessed November 2005).

NARUC/NRRI. 2003. Survey on Critical Infrastructure Protection. http://www.nrri.ohio-state.edu/dspace/bitstream/2068/296/1/04-01.pdf (accessed February 2, 2006).

National Aeronautics and Space Administration. 2003. Final Report of the Columbia Accident Investigation Board, 2003. http://www.caib.us (accessed June 3, 2006).

National Center for Infectious Diseases. 1999. Emerging Infectious Diseases. In *Special Issue on Bioterrorism.* Atlanta, GA: Centers for Disease Control.

National Commission on Terrorism. 2000. Countering the Changing Threat of International Terrorism (Bremer Report). Washington, DC: National Commission on Terrorism.

National Commission on Terrorist Attacks upon the United States. 2004. The 9/11 Commission Report. Washington, DC: Government Printing Office. http://www.9-11commission.gov/report/911Report.pdf (accessed February 25, 2006).

National Council on Public Works Improvement. 1988. Fragile Foundations: A Report on America's public Works. Final Report to the President and Congress. Washington, DC.

National Infrastructure Simulation and Analysis Center. 2003. Defense Treat Reduction Agency Program Review. Arlington, VA.

National Institute of Standards and Technology. 1995. The Impact of the FCC's Open Network Architecture on NS/NP Telecommunications Security Washington DC: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-11/titleona.html (accessed May 7, 2003).

National Research Council. 2002a. *Cybersecurity Today and Tomorrow: Pay Now or Pay Later.* Washington, DC: National Academies Press.

National Research Council. 2002b. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism.* Committee On Science and Technology for Countering Terrorism Washington, DC: National Academies Press.

National Security Telecommunications Advisory Committee. 2002. Network Security/Vulnerability Assessments Task Force Report. Washington, DC: President's National Security Telecommunications Advisory Committee. http://www.ncs.gov/nstac/reports/2002/NSVATF-Report-(FINAL).htm (accessed March 6, 2006).

National Task Force on Interoperability. 2003. "Why Can't We Talk? Working Together To Bridge the Communications Gap To Save Lives. National Institute of Justice. http://www.ojp.usdoj.gov/nij/topics/commtech/ntfi_guide.pdf (accessed March 27, 2006).

National Transportation Safety Board. 2006a. Rail Accidents 2006. http://ntsb.gov/Publictn/R_Acc.htm. (accessed March 10, 2006).

National Transportation Safety Board. 2006b. Train Crew Failed to Reline Main Line Switches and Causes Collision and Derailment in South Carolina NTSB Finds. November 29. http://www.ntsb.gov/Pressrel/2005/051129.htm (accessed March 10, 2006).

National Vulnerability Database. 2005. CVE Vulnerability Search Engine. http://nvd.nist.gov/statistics.cfm (accessed February 22, 2006).

Neuman, P. 1991. NY Area Fiber-Optic Telephone Cable Severed; Extensive Effects. *The Risk Digest.* http://catless.ncl.ac.uk/Risks/10.75.html#subj1 (accessed May 7, 2003).

Neuman, P. 2000. Week-long outage after cable cut downs 11,000 phone lines. *The Risk Digest 20:84.* http://catless.ncl.ac.uk/Risks/20.84.html#subj6.1 (accessed May 7, 2003).

New York Times. 2003. Northeastern United States and Canada power blackout, August 14, 2003, p. A1.

Newman, R. 2002. Wall Street Worries. *U.S. News & World Report,* September 23, 46–48.

Nickel, B., and D. Wilkinson. 1983. Invasion Percolation on the Cayley Tree: Exact Solution of a Modified Percolation Model. *Physical Review Letters* 51(2): 71–74.

North American Electric Reliability Council. 2001. System Disturbance Reports. Disturbance Analysis Working Group, review of Selected Electric System Disturbances in North America, 1996, 1998, and 2001. Princeton, NJ: NERC. http://www.nerc.com/~filez/dawg-disturbancereports.html (accessed February 8, 2006).

North American Electric Reliability Council. 2006. System Disturbance Reports. Disturbance Analysis Working Group 2001. http://www.nerc.com/~filez/dawg-disturbancereports.html (accessed February 8, 2006).

Norton, B. 1982. Environmental Ethics and the Rights of Future Generations. *Environmental Ethics* Winter: 319–338.

O'Hanlon, M. E., P. R. Orszag, I. H. Daalder, I. M. Destler, D. L. Gunter, R. E. Litan, and J. B. Steinberg. 2002. Protecting the American Homeland: A Preliminary Analysis. Chapter 6: Principles for Providing and Financing Homeland Security. Washington, DC: Brookings Institution. http://www.brookings.edu/fp/projects/homeland/fullhomeland.pdf (accessed February 2, 2006).

Office of Homeland Security. 2002. National Strategies for Homeland Security. Washington, DC: Office of the President.

Office of Management and Budget. 2004. Budget of the United States Government, Fiscal Year 2004, Historical Table 1–2. http://www.whitehouse.gov/news/usbudget/budget-fy2004/hist.html (accessed March 4, 2006).

Office of the President. 1998. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. White paper. May 22. http://www.usdoj.gov/criminal/cybercrime/white_pr.htm (accessed November 2005).

Office of the President. 2003. National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Washington, DC.

Organization for Economic Cooperation and Development. 2005. Terrorism Insurance in OECD Countries. July 5. Paris: OECD.

Ortolani, Alex, and Robert Block. 2005. Keeping Cargo Safe From Terror: Hong Kong Port Project Scans All Containers; U.S. Doesn't See the Need. *Wall Street Journal,* July 29, B1.

Paine, Thomas. 1776. *Common Sense.* http://www.alumni.uchicago.edu/commontext/paine/documents/CommonSense.pdf (accessed February 25, 2006).

Papadakis, I. S., and W. T. Ziemba. 2001. Derivative Effects of the 1999 Earthquake in Taiwan to U.S. Personal Computer Manufacturers. In *Mitigation and Financing of Seismic Risks,* edited by P. R. Kleindorfer and M. R. Sertel. Boston: Kluwer Academic Publishers.

Perrings, C. 1991. Reserved Rationality and the Precautionary Principle: Technological Change, Time and Uncertainty in Environmental Decision Making. In *Ecological Economics: The Science and Management of Sustainability,* edited by R. Costanza. New York: Columbia University Press.

Perrow, C. 1984. *Normal Accidents: Living with High-Risk Technologies.* New York: Basic Books.

Perrow, C. 1999. *Normal Accidents.* Princeton, NJ: Princeton University Press.

Peters, Guy B. 1998. Managing Horizontal Government: The Politics of Coordination: Canadian Centre for Management Development, Minister of Supply and Services.

Peters, Ralph. 1999. *Fighting for the Future: Will America Win?* Mechanicsburg, PA: Stackpole Books.

Philippsohn, S. 2001. Trends in Cybercrime – An Overview of Current Financial Crimes on the Internet. *Computers & Security* 20(1): 53–69.

Phillips, Lord, J. Bridgeman, and M. Ferguson-Smith. 2000. The BSE Inquiry, vol 1. Findings and Conclusions. October, section 1176. London: Stationary Office.

Phimister, James R., Vicki M. Bier, and Howard C. Kunreuther (eds.). 2004. *Accident Precursor Analysis and Management: Reducing Technological Risk Through Diligence.* Washington, DC: National Academy of Engineering.

Pidgeon, Nick, Roger Kasperson, and Paul Slovic (eds.). 2003. *The Social Amplification of Risk.* Cambridge, UK: Cambridge University Press.

Pillar, P. 2001. *Terrorism and U.S. Foreign Policy.* Washington, DC: Brookings Institution Press.

Posner, Gerald. 2003. *Why America Slept.* New York: Random House.

Posner, Richard A. 2004. *Catastrophe: Risk and Response.* New York: Oxford University Press.

Potok, M. 2004. The American Radical Right: The 1990s and Beyond. In *Western Democracies and the New Extreme Right Challenge,* edited by R. Eatwell and C. Mudde. Oxford, UK: Routledge.

President's Commission on Critical Infrastructure Protection. 1997. Critical Foundations, Protecting America's Infrastructures. Washington, DC.

President's Council of Advisors on Science and Technology. 2002. Report on Maximizing the Contribution of Science and Technology Within the new Department of Homeland Security.

President's Council of Science and Technology Advisors. 2003. The Science and Technology of Combating Terrorism.

Pressman, J. L., and A. Wildavsky. 1984. *Implementation.* 2nd ed. Berkeley, CA: University of California Press.

PSERC. 2003. Public Utilities of Commission of Ohio, sequence of events on August 14. http://www.pserc.wisc.edu/Ohio_Only_Sequence_of_Events.pdf (accessed December 7, 2003).

Ralyea, Harold C., and Jeffrey W. Seifert. 2004. Information Sharing for Homeland Security: A Brief Overview. September 30, RL32597. Washington, DC: Congressional Research Service, 22–25.

Reason, J. 1997. *Managing the Risks of Organizational Accidents.* Hampshire, England: Ashgate Publishing Company.

Rees, Joseph. 1996. *Hostages of Each Other: The Transformation of Nuclear Safety since Three Mile Island.* Chicago: University of Chicago Press.

Rees, T. 1994. *Hostages to Each Other.* Chicago: University of Chicago Press.

Regalado, A., and G. Fields. 2003. Blackout a Reminder of Grid's Vulnerability to Terror. *Wall Street Journal,* August 15.

Reisner, Robert. 2002. Homeland Security Brings Ratepayers vs. Taxpayers to Center Stage. In *Postal and Delivery Services. Delivering on Competition,* edited by Crew and Kleindorfer. Boston: Kluwer Academic Publishers.

Renesys. 2003. Blackout Results in Widespread Network Outages. August 14. http://www.renesys.com/news/index.html (accessed December 7, 2003).

Renz, Loren, Elizabeth Cuccaro, and Leslie Marino. 2003. *9/11 Relief and Regranting Funds: A Summary Report on Funds Raised and Assistance Provided.* New York: Foundation Center, December.

Revised Draft National Infrastructure Protection Base Plan. 2006. Version 2.0 January. http://cryptome.org/nipp-v2.zip (accessed March 8, 2006).

Risen, James, and Eris Lichtblau. 2005. Bush Lets U.S. Spy on Callers Without Courts. *New York Times* http://www.nytimes.com/2005/12/16/politics/16program.html?ex=1292389200&en=e32072d786623ac1&ei=5090&partner=rssuserland&emc=rss (accessed March 14, 2006).

Rittel, Horst, and Melvin Webber. 1973. Dilemmas in a General Theory of Planning. *Policy Sciences* 4: 155–169.

Rivlin, Gary. 2005. New Orleans Utility Struggles To Relight a City of Darkness. *New York Times,* New York City edition, Nov. 19, A1.

Roberts, H. K., and C. Libuser. 1993. From Bhopal to Banking: Organizational Design can Mitigate Risk. *Organizational Dynamics* 21: 15–26.

Roberts, Karlene. 1990a. Managing High Reliability Organizations. *California Management Review* 32, 4: 101–114.

Roberts, K. H. 1990b. Some Characteristics of High Reliability Organizations. *Organization Science* 1(2): 160–177.

Roberts, K. H. 1993. Some Aspects of Organizational Cultures and Strategies to Manage Them in Reliability Enhancing Organizations. *Journal of Managerial Issues* 5: 165–181.

Roberts, K. H., and G. Gargano. 1989. Managing a High Reliability Organization: A Case for Interdependence. In *Managing Complexity in High Technology Industries: Systems and People,* edited by M. A. VonGlinow and S. Mohrmon. New York: Oxford University Press.

Roberts, Nancy. 2001. Coping with Wicked Problems: The Case of Afghanistan. In *Learning from International Public Management Reform,* Vol. 11B. Amsterdam: Elsevier Science Ltd.

Rochlin, G. I. 1993a. Defining High Reliability Organizations in Practice. In *New Challenges to Understanding Organizations,* edited by K. Roberts. New York: Macmillan.

Rochlin, G. I. 1993b. *Trapped in the Net: the Unanticipated Consequences of Computerization.* Princeton, NJ: Princeton University Press.

Rochlin, G. I. 1996. Reliable Organizations: Present Research and Future Directions. *Journal of Crisis and Contingency Management* (Issue on High Reliable Organization Research) 4(2): 55–59.

Rochlin, G. I. 1999. Safe Operations as a Social Construct. *Ergonomics* 42(11): 1549–1560.

Rochlin, G. I. 2001. Highly Reliable Organizations: Exploration and Research Perspectives. In *Organiser la Fiabilite,* edited by M. Bourrie. Paris: L'Harmattan.

Rochlin, G. I., and A. von Meier. 1994. Nuclear Power Operations: A Cross-Cultural Perspective. *Annual Review of Energy and the Environment* 19: 153–187.

Rochlin, G. I., Todd R. LaPorte, and Karlene H. Roberts. 1987. The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea. *Naval War College Review* 76–90.

Roe, E., M. J. G. van Eeten, P. R. Schulman, and M. de Bruijne. 2002. California's Electricity Restructuring: The Challenge to Providing Service and Grid Reliability. Palo Alto, CA: California Energy Commission, Lawrence Berkeley National Laboratory, and the Electrical Power Research Institute.

Roe, E., P. Schulman, M. J. G. van Eeten, and M. deBruijne. 2005. High Reliability Bandwidth Management: Findings and Implications of Two Case Studies. *Journal of Public Administration Research and Theory* 15: 263–280.

Saleh, Mohamad. 2003. Al Qaeda Claims Responsibility for Power Blackout in U.S.! *Dar Al Hayat,* August 18. http://english.daralhayat.com/arab_news/08-2003/Article-20030818-14bdd659-c0a8-01ed-0079-6e1c903b7552/story.html (accessed October 21, 2003).

Sandler, T., and W. Enders. 2004. An Economic Perspective of Transnational Terrorism. *European Journal of Political Economy* 20(2): 301–316.

Sarkar, Dibya. 2004. DOJ Writes to Share. *Federal Computer Week*, October 15. http://www.fcw.com/fcw/articles/2004/1011/web-doj-10-15-04.asp (accessed November 2005).

Scalfane, Susanne. 2006. Unexpected Surplus Climb: Despite Storms, Industry Profits Rise, National Underwriter P&C. January 2/9, 110, 1. http://cms.nationalunderwriter.com/cms/NUPC/Weekly%20Issues/Issues/2006/01/News/P01ISONINE-ss?searchfor=despite%20storms%20january%202006 (accessed March 4, 2006).

Schein, E. H. 1994. Organizational and Managerial Culture as a Facilitator or Inhibitor of Organizational Learning. http://www.solonline.org/res/wp/10004.html.

Schelling, T. 1978. *Micromotives and Macrobehavior.* New York: Norton Interdependent Security.

Schratz, P. R. 1983. Admiral Rickover and the Cult of Personality. *Air University Review*, July–August. http://airpower.maxwell.af.mil/airchronicles/aureview/1983/jul-aug/schratz.html (accessed June 27, 2006).

Schulman, Paul R. 1993a. The Analysis of High Reliability Organizations: A Comparative Framework. In *New Challenges to Organization Research: High Reliability Organization*, edited by K. H. Roberts. New York: Macmillan.

Schulman, P. R. 1993b. A Comparative Framework for the Analysis of High Reliability Organizations. In *New Challenges to Understanding Organizations*, edited by K. Roberts. New York: Macmillan.

Schulman, P. R. 1993c. Negotiated Order of Organizational Reliability. *Administration and Society* 25(3): 356–372.

Schulman, P. R. 2002. Medical Errors: How Reliable Is Reliability Theory? In *Medical Error: 200–216*, edited by M. M. Rosenthal and L. M. Sutcliffe. San Francisco, CA: Jossey-Bass.

Schulman, Paul R., and Emery Roe. 2004. Managing for Reliability in an Age of Terror. Paper presented at Private Efficiency, Public Vulnerability Workshop, Cambridge, MA, May 28.

Schulman, P. R., E. Roe, M. van Eeten, and M. de Bruijne. 2004. High Reliability and the Management of Critical Infrastructures. *Journal of Contingencies and Crisis Management* 12(1): 14–28.

Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. 2006. A Failure of Initiative. U.S. House of Representatives. http://katrina.house.gov/full_katrina_report.htm (accessed March 23, 2006).

Seligman, A. 2000. *The Problem of Trust.* Princeton, NJ: Princeton University Press.

Seltzer, L. 2004. Who Wrote Sobig? eWeek. http://www.eweek.com/article2/0,1759,1716992,00.asp (accessed December 7, 2005).

Selznick, P. 1957. *Leadership in Administration.* New York: Harper & Row.

Sherman, Mark. 2005. Subway Threat Puzzle: When Local Officials, Feds Disagree. *Associated Press.* October 7. http://www.nctimes.com/articles/2005/10/08/news/nation/15_32_5810_7_05.txt (accessed November 2005).

Short, T. 2002. Reliability Indices. Conference report, T&D World Expo 2002, Indianapolis, IN, May 7–9, 2002. http://www.epri-peac.com/td/pdfs/reliability2002.pdf (accessed March 25, 2006).

Shrader, R., and R. J. Woolsey. 2002. Business Has To Be Involved in Security Planning. *Financial Times*, January 16.

Shrader-Frechette, K. 1993. Risk Methodology and Institution Bias. *Research in Social Problems and Public Policy* 5: 207–223.

Simon, Steven, and David Benjamin. 2005. *The Next Attack.* New York: Henry Holt & Company.

Singel, Ryan. 2005a. Passenger Screening, Take 10. Wired News. January 31. http://www.wired.com/news/privacy/0,1848,66433,00.html?tw=wn_story_related (accessed November 2005).

Singel, Ryan. 2005b. Secure Flight Hits Turbulence. *Wired News.* June 15. http://www.wired.com/news/privacy/0,1848,67875,00.html?tw=wn_story_related (accessed November 2005).

Singer, Peter. 2002. *Corporate Warriors.* Washington, DC: Brookings Institution Press.

Slovic, P. 1993. Perceived Risk, Trust, and Democracy. *Risk Analysis* 13(6): 675–682.

Slovic, P. 1999. Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield. *Risk Analysis* 19(4): 689–701.

Slovic, Paul. 2000. *The Perception of Risk.* London: Earthscan Publications.

Smetters, K. 2004. Insuring Against Terrorism: The Policy Challenge. In *Brookings-Wharton Papers on Financial Services*, edited by R. Litan and R. Herring, 139–182.

Sood, Sunil K. 2004. Food Poisoning. eMedicine. http://www.emedicine.com/ped/topic795.htm (accessed March 10, 2006).

Stacey, Ralph. 1996. *Strategic Management & Organizational Dynamics.* London: Pitman.

Starks, Tim, and Martin E. Andersen. 2004. Congress, Industry Both Dismay over Homeland Security's Performance on Critical Infrastructure. *CQ Homeland Security.*

State of New York Public Service Commission. 2005. CASE 04-E-0822 – In the Matter of Staff's Investigation into New York State's Electric Utility Transmission Right-of-Way Management Practices, filed in Case 27605. http://www3.dps.state.ny.us/pscweb/webfileroom.nsf/ArticlesByCategory/BDB52B0CC15BBE74852570260063242B/$File/301.04e0822.pdf?OpenElement (accessed February 9, 2006).

Stauffer, D., and A. Aharony. 1994. *Introduction to Percolation Theory.* London and New York: Routledge.

Stephenson, John B. 2005. Homeland Security: Federal and Industrial Efforts Are Addressing Security Issues at Chemical Facilities, but Additional Action Is Needed. Testimony by John B. Stephenson, U. S. Accountability Office, before the Committee on Homeland Security and Governmental Affairs, U. S. Senate, April 27.

Stern, J. 2003. *Terror in the Name of God: Why Religious Militants Kill.* New York: Harper Collins.

Strohm, Chris. 2004. Threat Warning Creates Confusion Over Homeland Security Roles. GovExec.com. http://www.govexec.com/dailyfed/0504/052804c1.htm (accessed November 2005).

Sturgeon W. 2003. Organized Crime behind Sobig – Virus Expert. http://news.zdnet.co.uk/internet/security/0,39020375,39115886,00.htm (accessed May 24, 2004).

Swiss Re. 2006. Natural Catastrophes and Man-Made Disasters in 2005. Sigma, N2. February.

Talukdar, S., J. Apt , M. Ilic, L. Lave, and M. G. Morgan. 2003. Cascading Failures: Survival vs. Prevention. *Electricity Journal* 16(9): 25–31.

Terrorism Risk Insurance Act of 2002, Pub. Law No. 107–297, 116 Stat. 2322; 31 C.F.R. Part 50. http://www.ustreas.gov/offices/domestic-finance/financial-institution/terrorism-insurance/ (accessed February 25, 2006).

Terrorist Risk Reinsurance Program. 2005. U.S. House of Representatives, July 1.

Thompson, William C. 2002. One Year Later: The Fiscal Impact of 9/11 on New York City. http://comptroller.nyc.gov/bureaus/bud/reports/impact-9-11-year-later.pdf (accessed February 25, 2006).

Tillinghast-Towers Perrin. 2002. September 11, 2001: Implications for the Insurance Industry, Towers Perrin Reinsurance, T193-01, September 21, 2001. New York: Tillinghast-Towers Perrin. http://www.towersperrin.com/tillinghast/publications/reports/Sept_11_Implications_For_Insurance/2002051310.pdf (accessed January 10, 2006).

Time Magazine. 1977. Night of Terror. July 25. 12–26.

Transmission & Distribution World. 2005. AREVA to Build De-Icing and Power-Quality System. http://tdworld.com/mag/power_areva_build_deicing (accessed February 8, 2006).

Transportation of Highly Reliable Organizations: Past Research and Future Explorations. 1999. Paper presented at Workshop on Approaches to Organizational Reliability, October 7–8, at Department Technologies et Sciences de l'Homme, Universite de Technologies de Compiegne, France.

Tuchman, Barbara. 1962. *The Guns of August.* Toronto: Bantam.

Tucker, Jonathan B. 1999. Historical Trends Related to Bioterrorism: An Empirical Analysis. National Symposium on Medical and Public Health Response to Bioterrorism. Emerging Infectious Diseases, July–August, 5(4): 498–504.

Tucker, Jonathan B., and Amy Sands. 1999. An Unlikely Threat. *Bulletin of the Atomic Scientists* 55(4).

Turner, Barry A. 1976. The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly* 21(3): 378–397.

Turner, Barry A. 1978. *Man-Made Disasters: The Failure of Foresight.* New York: Crane, Russak.

Turner, Barry A., and Nick F. Pidgeon. 1997. Man-Made Disasters. 2nd ed. Oxford, United Kingdom Butterworth-Heinemann.

U.S. Congress. 2002. Terrorism Risk Insurance Act of 2002. HR 3210 (became Pub. L. 107–297, 116 Stat. 2322). http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ297.107.pdf (accessed March 20, 2006).

U.S. Department of Justice. 1988. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. White Paper, May 22. http://www.usdoj.gov/criminial/cybercrime/white_pr.htm (accessed November 2005).

U.S. Department of State. 2004. Global Patterns in Terrorism. Washington, DC: Office of the Coordinator for Counterterrorism.

U.S. Department of State. 2005. Country Reports on Terrorism. Released by the Office of the Coordinator on Counterterrorism, April 27. http://www.state.gov/s/ct/rls/45321.htm (accessed January 12, 2006).

U.S. Department of the Treasury. 2005. Assessment: The Terrorism Risk Insurance Act of 2002. Washington, DC: Office of Economic Policy. June 30.

U.S.–Canada Power System Outage Task Force. 2004. Final Report on the August 14, 2003, Blackout in the United States and Canada: Causes and Recommendations. April 5. Washington, DC: U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability.

Van Eeten, M. J. G., E. M. Roe, P. Schulman, and M. L. C. de Bruijne. 2006. The Enemy Within: System Complexity and Organizational Surprises. In *International CIIP Handbook 2006 Vol. II Analyzing Issues, Challenges, and Prospects,* edited by M. Dunn and V. Mayer. Zurich: Center for Security Studies of the ETH Zurich, 89–109.

Vegh, S. 2002. Activists or Cyberterrorists? The Changing Media Discourse on Hacking. *Firstmonday 7:10.* http://www.firstmonday.dk/issues/issue7_10/vegh/ (accessed May 7, 2003).

Verton D. 2003. *Black Ice: The Invisible Threat of Cyber-Terrorism.* New York: McGraw-Hill Osborne Media.

Wall Street Journal. 2005. A Massive Repair Job Begins To Fix Gulf's Broken Oil Network. September 8.

Watts, D. 2003. Security and Vulnerability in Electric Power Systems. Proceedings of the 35th North American Power Symposium, University of Missouri-Rolla, October 20–21, 559–566.

Weber, Max. 1946. Politics as a Vocation. In *From Max Weber: Essays in Sociology,* edited by H. H. Gerth and C. Wright Mills. New York: Oxford University Press.

Wedgwood, R. 2002. Al Qaeda, Terrorism, and Military Commissions. *American Journal of International Law* 96(2): 328–337.

Weick, K. E. 1987. Organizational Culture as a Source of High Reliability. *California Management Review* 29: 112–127.

Weick, Karl, and Kathleen Sutcliffe. 2001. *Managing the Unexpected: Assuring High Performance in an Age of Complexity.* University of Michigan Business School Management Series. San Francisco, CA: Jossey-Bass.

Weick, K. E., K. M. Sutcliffe, and D. Obstfeld. 1999. Organizing for High Reliability: Quantitative and Qualitative Assessment Aboard Nuclear Powered Aircraft Carriers. *Journal of High Technology Management Research* 5(1): 141–161.

Weisstein, Eric W. 1999. Cayley Tree. In *MathWorld – A Wolfram Web Resource.* http://mathworld.wolfram.com/CayleyTree.html (accessed June 27, 2006).

Wenz, P. 1983. Ethics, Energy Policy, and Future Generations. *Environmental Ethics* 5: 195–209.

Western Systems Coordinating Council. 1996. Disturbance Report for the Power System Outage that Occurred on the Western Interconnection, August 10. 1548 PAST, Published October 18, 1996.

Wharton Risk Management and Decision Processes Center. 2005. TRIA and Beyond. Wharton School, University of Pennsylvania, Philadelphia p. 208. http://grace.wharton.upenn.edu/risk/downloads/TRIA%20and%20Beyond.pdf (accessed February 25, 2006).

White House. 1998. Protecting America's Critical Infrastructure: PDD 63 Fact Sheet. Washington, DC.

White House. 2002. National Strategy for Homeland Security. Washington, DC, July.

White House. 2003a. Homeland Security Presidential Directive/HSPD-7. December 17. http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html (accessed November 2005).

White House. 2003b. The National Strategy to Secure Cyberspace Washington, DC: White House Critical Infrastructure Protection Board. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (accessed December 3, 2003).

White House. 2004a. President Bush Celebrates Independence Day, West Virginia Capitol Grounds. http://www.whitehouse.gov/news/releases/2004/07/20040704.html (accessed January 12, 2006).

White House. 2004b. Remarks by the Vice President at the 123rd Coast Guard Academy Commencement. http://www.whitehouse.gov/news/releases/2004/05/20040519-5.html (accessed January 12, 2006).

White House. 2005a. Executive Order: Further Strengthening the Sharing of Terrorism Information to Protect Americans. http://www.whitehouse.gov/news/releases/2005/10/20051025-5.html (accessed November 2005).

White House. 2005b. The National Strategy for Homeland Security. July. http://www.whitehouse.gov/homeland/book/index.html (accessed July 12, 2006).

Wiening, Eric A. 2002. Foundations of Risk Management and Insurance. American Institute for Chartered Property and Casualty Underwriters/Insurance Institute of America, Malvern, PA.

Wiening, Eric A. 2002. *Foundations of Insurance Risk Management and Insurance.* AICPCU/IIA, 1st ed.

Wildavsky, Aaron. 1988. *Searching for Safety.* New Brunswick, NJ: Transaction Books.

Wilson, J. 2003. Blackout: The Conspiracy Theory. *Popular Mechanics* 180(11): 38, 40.

Wilson, J. Q. 1989. *Bureaucracy.* New York: Basic Books.

Wired. 2004. August 11. http://www.wired.com/news/print/0,1294,64168,00.html (accessed July 15, 2004).

World Health Organization. 2003a. SARS Outbreak Contained Worldwide. http://www.who.int/mediacentre/news/releases/2003/pr56/en/ (accessed February 9, 2006).

World Health Organization. 2003b. Update 95 – SARS: Chronology of a Serial Killer. http://www.who.int/csr/don/2003_07_04/en/index.html (accessed February 9, 2006).

Yoran, Amit. 2004a. Locking Your Cyber Front Door – the Challenges facing Home Users and Small Businesses. Statement of the Director, National Cyber Security Division, Office of Infrastructure Protection, U.S. Department of Homeland Security before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, U.S. House of Representatives, June 16.

Yoran, Amit. 2004b. Virtual Threat, Real Terror: Cyberterrorism in the 21st Century. Statement before the Senate Committee on the Judiciary Subcommittee on Terrorism, Technology and Homeland Security, February 24.

Yoshihara, T. 2001. Chinese Information Warfare: A Phantom Menace or Emerging Threat? *Strategic Studies Institute.* http://www.iwar.org.uk/iwar/resources/china/iw/chininfo.pdf (accessed May 7, 2003).

Zerriffi, H. 2004. Electric Power Systems Under Stress: An Evaluation of Centralized versus Distributed System Architectures. PhD Dissertation, Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, PA. http://wpweb2k.gsia.cmu.edu/ceic/theses/Hisham_Zerriffi_PhD_Thesis_2004.pdf.

Zipf, G. K. 1929. Relative frequency as a determinant of phonetic change. *Harvard Studies in Classical Philology* 15: 1–95.

Zipf, G. K. 1965. *Psycho-biology of Languages.* Cambridge, MA: MIT Press.

Zuboff, Shoshana. 1988. *In the Age of the Smart Machine.* New York: Basic Books.