Annu. Rev. Polit. Sci. 2005. 8:335–56
doi: 10.1146/annurev.polisci.8.081404.075608

First published online as a Review in Advance on Mar. 17, 2005

RISK, SECURITY, AND DISASTER MANAGEMENT

Louise K. Comfort
Graduate School of Public and International Affairs, University of Pittsburgh, Pittsburgh, Pennsylvania 15260; email: comfort@gspia.pitt.edu

Key Words uncertainty, resilience, networks, information asymmetry, adaptive learning

■ **Abstract** This review examines the policies and practices that address the evolving conditions of risk, security, and disaster management in U.S. society. Although each condition presents particular challenges to public agencies and the communities they serve, all represent varying states of uncertainty and require different approaches for informed action. This analysis reframes the issue of managing risk by focusing on the distinction between policies and practices developed in reference to natural and technological hazards and those developed to enhance security from hostile acts. The author concludes that building networks of organizations committed to a process of continual inquiry, informed action, and adaptive learning is a more flexible, robust strategy than the standard practice of establishing greater control over possible threats through administrative structures. Supported by methods of network analysis, computational simulation, information infrastructure, and long-term policy goals, networked strategies offer an important alternative to hierarchical structures that prove vulnerable in uncertain environments.

INTRODUCTION

The last three years have seen a striking change in the ways in which citizens perceive and respond to sudden, urgent, destructive events and, more importantly, in citizen expectations of the government's capacity to anticipate and respond to such events. The sobering and painful events of September 11, 2001 initiated a critical review of government performance, both before and after the disaster, and triggered a plethora of new policies, procedures, and a reorganization of government functions to make the United States—and, presumably, the world—safer. The result has been a blurring of existing disaster management policies and practices that had been largely oriented toward mitigating and recovering from natural disasters and technical failures—earthquakes, floods, severe winds, fire, hazardous materials releases, and transportation accidents—with policies developed to prevent deliberate disasters initiated by human intent to do harm, such as terrorism, arson, and chemical/biological releases.

More than three years after 9/11, it is possible to gain some perspective on the measures that have been taken in response to deliberate threats and to weigh the

changes these measures have created in the capacity of local, state, and national governments to manage the risk of continuing threats from natural and deliberate hazards. In some instances, these measures were indeed constructive and necessary. In other instances, they proved to be clumsy efforts that primarily distracted already overburdened local response agencies from the daily management of risk. In still other instances, such as the passage of the U.S.A. Patriot Act, the measure appeared to threaten the very freedoms the law was designed to protect.

This review considers recent articles, reports, and books that address the question of security versus sustainable management of risk and disaster. In his 1988 book, *Searching for Safety*, Aaron Wildavsky frames this question as he seeks to identify the appropriate balance between anticipating risk and generating resilience in response to disaster. This review will also address new methodological approaches to anticipating risk, including network analysis and computational modeling as a means of generating credible scenarios for action under known constraints of resources and law. These methods provide a way to anticipate natural, technological, or deliberate threats that government agencies have not seriously considered before. In important ways, these methods of research are changing the perceptions, policies, and practice of managing risk and disasters over extended periods.

The dialogue between risk and security will continue. By developing new concepts, methods, and skills to reframe old questions of safety, security, and disaster management, academicians can contribute to the sustainable management of continuing risk.

COPING WITH UNCERTAINTY

The quintessential role of government is to protect its citizens from harm. This role, widely accepted and understood for over two centuries in the United States, has led to a series of public policies and government actions that were designed to anticipate risk, prepare citizens to manage risk, and assist them in recovering from damaging events (May 1985, May & Williams 1986). These policies and procedures, however, assume that the government itself remains intact and that citizens are the unintended victims of destructive events. The rationale underlying these policies is that the government's primary role is to pool resources from the wider society as a means of reducing the uncertainty and adverse impact from potentially extreme events. This formulation is based on the interpretation of extreme events as largely probabilistic occurrences that lay outside the control of individual citizens.

Since the mid-1980s, however, more careful documentation of losses from disaster events and more critical analyses of government practice in disaster operations have led to a different formulation of the problem of extreme events. Disaster was viewed as a problem that could be managed more effectively by informed action and appropriate investment of attention and resources in risk-prone communities

(McLoughlin 1985, Comfort 1988). At local, state and federal levels of jurisdiction, governments were regarded as the primary actors in mobilizing communities to engage in the mitigation of risk and preparedness for possible disaster. These activities, in turn, would increase the capacity of communities to respond effectively when extreme events did occur and to recover more quickly from the damage. This assessment reshaped the problem of harm from extreme events as a probabilistic occurrence beyond ordinary human control to one in which human actions and changing social, economic, physical, and political conditions contributed significantly to creating vulnerability to damaging events (Platt 1999, Mileti 1999). In this conception, extreme events were less random occurrences beyond human control than products of inadequate planning, negligence, or uninformed actions that led to cumulative failure of human and engineered systems exposed to recurring risk (Comfort et al. 1999, Comfort 1999). The challenge was to manage these recurring events, and government agencies were viewed as primarily responsible for designing appropriate policies and enabling citizens to take informed action to reduce risk.

The events of 9/11 significantly altered both the public perception of risk and government's role in reducing or managing this risk. Although terrorism was not a new form of attack on the U.S. government, the coordinated attacks on the World Trade Center and the Pentagon represented the most damaging attacks by foreign enemies on U.S. soil since the Japanese attack on Pearl Harbor in 1941. Even more devastating than the colossal damage inflicted on the civilian targets of the World Trade Center was the perception that the existing government policies to protect citizens from such an attack were inadequate or dysfunctional. The response to this sobering event was immediate, and the U.S. public was united in its commitment to prevent such attacks from occurring ever again.

The difficulty, however, lay in determining exactly how to prevent attacks that were conducted by an elusive network of like-minded individuals who were accountable to no nation-state and who were determined to discredit the efficacy of the U.S. government by attacking its citizens. The security of U.S. citizens as they engaged in routine activities on an ordinary day had been breached. The event itself indicated a failure of government policies to manage the risk of deliberate attack, but it was not at all clear in the immediate aftermath of the event what policies should be corrected or changed.

Designing Policy for Different States of Uncertainty

Clearly, different categories of harm can befall citizens, and different government actions can be taken to reduce these potential harms. But the basic issue in designing appropriate public policy and strategies for action lies in determining the source and degree of uncertainty that characterize potential harms. Risk, security, and disaster represent different states of uncertainty in reference to damaging events. Designing public policy for each state requires different allocations of attention, resources, organizational structure, methods, and measurement of performance.

Risk represents the possible occurrence of a harmful event that has some known likelihood of happening over time. Disaster represents the interdependent cascade of failure triggered by an extreme event that is exacerbated by inadequate planning and ill-informed individual or organizational actions. Security, however, includes government actions taken to prevent the potential for deliberate harm and, as such, it acknowledges the hostile intent of the perpetrator(s) against both citizens and government. Each type of uncertainty represents a type of low-probability, high-consequence event that challenges government performance and civic tolerance for failure. How policy makers should manage such events and make trade-offs in practice regarding the costs or benefits for government (in)action in deeply uncertain contexts is a continuing challenge.

In his thoughtful book, *Searching for Safety*, Wildavsky (1988) framed the issue as risk versus resilience. To Wildavsky, risk was ever present in a complex social world, and it would be impossible for any government to eliminate risk altogether. Rather, he acknowledged that society chooses the risks to be minimized and accepts the remainder, knowingly or not. Wildavsky viewed risk as the ability to anticipate a damaging event and to take proactive steps to reduce that risk, knowing that there was still some likelihood that the event could occur. This known likelihood, or probability of occurrence, was considered acceptable risk, or that amount of risk considered too infrequent to worry about or too costly to avoid. Although Wildavsky's formulation does not solve the problem of designing government policies for managing risk, it does frame the issue in dynamic terms. The degree of risk varies under different conditions, and governments can design policies to reduce risk and increase security for a price measured in economic or political terms. Conversely, governments can relax security and increase risk as conditions change. Wildavsky's lasting insight on this problem is that the degree of risk that a society accepts in an uncertain environment is a matter of choice. The likely error, in his judgment, lies in the validity of the information, or lack of same, on which the choice is based.

Increasing Vulnerability of Complex Systems to Extreme Events

The events of 9/11 and the anthrax attacks in the months that followed vividly illustrate the trends of the increasing vulnerability of civilian societies to hostile actors and to the harmful usurpation of interdependent services designed to facilitate global exchange in transportation, communications, commercial activity, and other regional services. This vulnerability is related to the increasing use of technology that makes possible the rapid exchange of goods, services, people, information, and knowledge at an ever-decreasing cost to a wider group of the world's population. Simultaneously, the global population lags in developing the shared values and goals to manage this technology responsibly, and it lacks mechanisms to minimize the risks engendered from human error, misjudgment, malfunction, and mal-intent. These risks lead to deliberate disaster, with sobering

consequences for unprepared or ill-informed populations. Finding new methods of coping with deliberate disaster and discovering means to reduce security risks for civilian populations are primary challenges that cannot be ignored. This task represents a shared risk in which government agencies, private businesses, and nonprofit organizations must share the responsibility for taking informed action (Comfort 1999).

POLICY VS. PRACTICE IN MAINTAINING SECURITY

The intent of policy is to guide practice, but the reverse appears more consistently true. That is, good policy derives from practice. Yet this maxim is confounded in extreme events when there has been no previous incident that approximates the scale or scope of danger confronting public managers. This inability to imagine attacks on the security of U.S. cities on the scale of the 9/11 events limited government capacity to plan defensively for such threats. Government planning did occur, but it fell regrettably short of meeting the needs for coordinated action to protect the security of U.S. cities. To understand how this gap occurred and to design better strategies for improving government performance under security threats, it is useful to review the policies that were in place before 9/11, the policies that were put in place immediately after 9/11, and the reasoning underlying both strategies.

Policies Existing Before September 11, 2001

In the years immediately preceding 9/11, policy makers recognized the risk of terrorist attacks, as they had occurred sporadically throughout the 1990s. The first attack on the World Trade Center on February 26, 1993, the bombings of the U.S. embassies in Nairobi, Kenya and Dar es Salaam, Tanzania on August 7, 1998, and the attack on the U.S.S. Cole in Port Aden, Yemen on October 12, 2000 all signaled deliberate actions to harm U.S. personnel and property. These events alerted U.S. officials to the need to re-examine the government's capacity to manage risk from terrorist events. These events were primarily directed toward U.S. assets overseas, but federal agencies recognized that different actors with different responsibilities would need to re-organize their activities to reduce the threat and coordinate response in the event of a domestic attack.

In an effort to manage the risk of terrorist threats to U.S. personnel and institutions, federal agencies implemented the United States Government Interagency Domestic Terrorism Concept of Operations Plan in February 2001 (United States Government, 2001). Under this plan, known informally as the ConPlan, two types of response operations were to be initiated simultaneously in the event of a terrorist attack. The first was crisis management, or the effort to identify and pursue the perpetrators of the incident. The U.S. Department of Justice (DOJ) was designated as the lead agency for crisis management, and it coordinated its work with other agencies involved in pursuing individuals who may have engaged in illicit

activity. These agencies included the Federal Bureau of Investigation (FBI); the Central Intelligence Agency (CIA), when international agents were involved; the Immigration and Naturalization Service (INS), which governed entry and exit of foreign nationals across U.S. borders; and the Bureau of Alcohol, Tobacco, and Firearms (ATF), which tracked the entry of illegal substances across U.S. borders. These agencies operated within the bounds of security required for a criminal investigation.

The second type of response to a terrorist attack was consequence management. This response included the immediate mobilization of search and rescue operations to save the lives of people harmed by the incident, the provision of disaster assistance to the people who suffered losses from the incident, and the recovery and reconstruction of the damaged communities. The Federal Emergency Management Agency (FEMA) had lead responsibility for consequence management, focusing first on lifesaving operations and second on assistance to the victims and recovery of the damaged community. Under the Federal Response Plan (FEMA 2000), eight federal agencies in addition to FEMA were designated to play lead roles in disaster operations, with 25 federal agencies assigned responsibilities under 12 specified emergency support functions (Comfort 2003). The lead agencies included the Department of Transportation (DOT), the National Communications Service (NCS), the Department of Defense (DOD), the U.S. Department of Agriculture (USDA), the Department of Health and Human Services (HHS), the Department of Housing and Urban Development (HUD), the Environmental Protection Agency (EPA), and the General Accounting Office (GAO). Two departments had dual emergency support functions: the USDA had the primary support function for firefighting, carried out by its sub-unit, the U.S. Forest Service (USFS), as well as responsibility for food; FEMA was responsible for information management as well as urban search-and-rescue operations. The American Red Cross (ARC), a nonprofit organization, was designated as the lead agency for mass care.

Under the ConPlan, the participating federal agencies retained their separate identities and distinct responsibilities for daily operations. The plan was intended to structure interagency coordination among federal agencies in the event of an extreme action directed against the nation. It did not specify responsibilities for coordination among state and local agencies that would respond to terrorist attacks, and it did not specify coordination of activities for the prevention of potential attacks. It was, however, the operations plan that was legally in effect on 9/11 (Comfort 2003).

Policies Implemented after September 11, 2001

The devastating consequences of the 9/11 terrorist attacks precipitated an almost immediate reaction to change government policy to increase security and reduce the danger of further terrorist attacks. Returning to Wildavsky's concept of the tension between risk and resilience in setting government policy, the balance in government action tipped in favor of reducing risk and against resilience as a

means of countering threats. The tolerance for risk in U.S. society dropped to near zero, as reflected by two major policy changes: the passage of the U.S.A. Patriot Act and the establishment of a cabinet-level Department of Homeland Security. These policies, grafted onto existing policies for mitigating risk and managing emergencies, were performed, in large part, by agencies with distinct missions, histories, and organizational cultures. Despite significant efforts to integrate these functions organizationally, the intended level of security and reduction of risk has not been achieved. The questions of how and why these efforts have failed merit examination.

The U.S.A. Patriot Act

Aggrieved by the failure of U.S. intelligence agencies to identify the evolving threat that culminated in the 9/11 attacks, the U.S. Congress and the president sought new ways of monitoring potential threats and securing U.S. borders and institutions against potential threats. The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (U.S.A. Patriot Act) Act of 2001" was passed by the 107th Congress and signed into law by President George W. Bush on October 26, 2001. Although the act includes a sunset provision that causes it to expire on December 31, 2005, the unusual powers granted to government agencies to conduct surveillance, intercept communications, extend searches, and hold information or persons who might be relevant to the search for terrorist activity without demonstrated evidence has raised significant questions regarding the power of the state to limit individual privacy in the name of increasing public security.

The U.S. Department of Homeland Security

Within weeks of 9/11, President George W. Bush established an Office of Homeland Security, and appointed Tom Ridge, then governor of Pennsylvania, to advise him on the development of a national strategy for homeland security. Governor Ridge accepted this position as Director of the White House Office on Homeland Security on October 6, 2001 and began an effort to organize a coordinated response among the federal agencies to increase their capacity for public security. In this position, he reported directly to the president but had no executive authority or budget. He could only advise, persuade, cajole, threaten, or negotiate agreements among the multiple federal agencies with differing responsibilities for border control, immigration, customs inspection, and intelligence gathering both within and outside the U.S. to share information and coordinate their activities. His first task was to identify which agencies performed what functions that were relevant to homeland security. The product of this analysis was a densely overlapping chart that identified 22 federal agencies with distinct responsibilities related to homeland security. The key issue, identified by Ridge as well as other informed analysts, was intergovernment coordination among not only these federal agencies, with their distinct cultures and competitive interests for budgets and personnel, but

also with the state and local agencies that shared responsibility for implementing a comprehensive national security strategy (Posner 2002).

The proposal for a cabinet-level Department of Homeland Security generated substantive debate both for and against this massive structural reorganization. Those in favor believed that the reorganization would bring all relevant agencies together under one shared mission and grant a senior cabinet-level executive the authority and budget to coordinate performance among them. They argued that a cabinet-level appointment was needed to gain and keep the attention of the president on these issues and to defend the national mission of securing the homeland against separate efforts to protect the identity and budgets of single agencies. Those who opposed the strategy, including initially the White House, argued that the individual agencies had distinctive capabilities that would be minimized in a larger, more complex organization. Further, the difficulty of integrating these disparate agencies would delay and distract them from performing their separate functions at expected professional levels, and it would take years to build trust and mutual understanding among them. Nonetheless, on January 23, 2003, President Bush signed Executive Order 13,284, which established the U.S. Department of Homeland Security.

Contrasting Practice

The test of a policy's effectiveness lies in its ability to transform practice. By this measure, the record is mixed regarding the effectiveness of these two major policies designed to reduce risk, increase security, and manage disaster more effectively and efficiently. Instead of reassuring citizens that their basic freedoms were being better protected, the U.S.A. Patriot Act has generated substantial resistance among citizens who worry that the powers of surveillance granted to the state are being misused for questionable purposes (Nelson 2002). Strongly held values of privacy and individual freedom gave rise to serious questions regarding the capacity of citizens to hold government authorities accountable for their exercise of powers authorized by the U.S.A. Patriot Act, including surveillance, wiretapping, and information sharing based on dubious intelligence-gathering activities.

As the principal investment in developing a national strategy for increasing public security, the Department of Homeland Security has not demonstrated its ability to change significantly the practice of the 22 agencies now gathered under its overarching framework. Although the agencies share the same email address @dhs.gov, they are nonetheless carrying out their basic functions largely independently, in arrangements that were negotiated with a carefully crafted goal of minimizing conflict and securing at least verbal collaboration among principals. Admittedly, the reorganization effort is a difficult task, and some work is indeed moving forward. Budgets are being allocated, although spending priorities have not always been congruent with security needs or implemented in a timely manner. Accurate assessments of existing capacities for security at both local and state levels have been difficult to obtain, and agencies frequently resort to familiar methods of political distribution in order to satisfy allocation deadlines.

The apparent incongruence between policies and practice regarding the development of an effective strategy for increasing public security compels a reexamination of the policies adopted. To a large extent, the policies designed and implemented followed time-honored government strategies of seeking greater control over the uncertainty generated by terrorist threats. By extending government control over citizen activity as a means of identifying potential terrorist threats, did governmental agencies alienate the very groups of citizens and organizations who could contribute most to reducing such threats? The number of foreign students seeking visas to study in the United States, for example, has declined significantly. Many of these students not only bring knowledge of the languages and cultures of nations in parts of the world that have generated terrorist groups, but they also have stayed in the United States after graduation and contributed substantially to the knowledge base of science and technology that is essential to U.S. economic proficiency. Although there has been no major terrorist attack within U.S. borders since 9/11, it is not evident whether the United States has the capacity to prevent or interrupt such an attack, despite $43.7 billion dollars of expenditures.

Clearly, the operational environment for detecting potential threats to public security has changed significantly. This environment is increasingly complex, dynamic, and adaptive in using sophisticated techniques of planning, technology, and biotechnology. Continuing terrorist threats show little sign of abatement, as documented by recent incidents in Indonesia, Spain, Saudi Arabia, Egypt, and Italy. These attacks appear to be orchestrated by networks of highly committed actors, operating freely across national boundaries and within the protection of legal jurisdictions. The standard approach of administrative hierarchy, adopted by the U.S. policies, appears mismatched to counter the flexible, stateless networks of organized terrorists in practice. More sobering is the compelling evidence presented in the 9/11 Commission Report (2004) that documents startling gaps in performance of government agencies and in the communication and coordination among them. Although the report reviews only the performance of agencies leading up to the 9/11 attacks, there is little evidence that the principal policies adopted by the U.S. since 9/11 have altered its basic approach of administrative hierarchy. The primary problem, as documented in the report, appeared to be the asymmetry of information among relevant organizations with shared risks and responsibilities. Government agencies, based on incomplete or untimely information, did not recognize the risks presented by seemingly ordinary, but highly interconnected, actions by terrorists operating in different locations. Given the nature of the threat—secretive, lethal, and ruthlessly ideological—the multijurisdictional administrative structure developed for responding to natural and technological disasters is largely inappropriate for networked threats that cross jurisdictional boundaries and target civilian populations. Despite acknowledgment of the need for increased collaboration and cooperation among agencies, governmental policy has relied instead on the creation of large structures for administrative control through the Department of Homeland Security. There is an urgent need for fresh concepts and new measures of government action in uncertain environments that can counter effectively the rapidly evolving, dynamic strategies of networked threats.

THE LOGIC OF UNCERTAINTY

If standard administrative structures prove too rigid to perform effectively against the dynamic and flexible networks of terrorists, what forms and conceptual frameworks could serve as constructive models? Returning to the documented experience of practicing disaster managers, several approaches are useful that could be incorporated or combined to inform administrative practice. Four of these approaches will be outlined briefly below. None is entirely new. Each is intended to reduce risk, and all four are familiar concepts to practicing decision-makers working in environments of uncertainty. The four approaches differ from standard administrative practice: all acknowledge that dynamic environments require learning processes that enable flexible adaptation and collective action rather than attempts to exert control through an administrative hierarchy of rules and constraints. In designing such systems, managers recognize the centrality of information flow among participating agents that include technical systems as well as human actors.

After Action Reviews

After field operations are concluded in any major disaster, it is standard practice for the operations chiefs to call for an "after action review." These events, also called "hot washes" in the vernacular of emergency service personnel, constitute a rigorous review of the operations just concluded. They are intended as a candid, thorough examination of actual operations to determine what went right, what went wrong, and how to improve performance before the next event. Emergency personnel know how difficult it is to manage complex operations in the urgent context of disaster. They also know that mistakes cost both lives and property and that their credibility with the communities they serve depends upon performance. They recognize that plans and standard operating procedures defined at one time in one context may not be the most effective means of managing a different incident in a different setting. Any disaster represents a failure of existing policy, and the critical objective of these reviews is to identify mistakes in operations in order to avoid making the same mistakes again. Differences between the existing policy and the actual conduct of operations serve as the basis for organizational change and continued learning. After action reviews represent a method of organizational learning that is taken very seriously by the participating personnel. These events provide a way to compare the organization's existing model of performance against the actual requirements of field operations. On this basis of collective review, recommendations for change in design, strategy, and tactics are incorporated into the organization's performance model for the next event.

Recognition-Primed Decision Making

Researchers from several disciplines have studied the process of decision making under stress (Weick 1995, Weick & Roberts 1993, Rochlin 1993, Flin 1996). Noting that decision making capacity often drops under stress (Flin 1997), several

researchers have observed that decision makers use models other than the standard rational model of assessing the problem, identifying alternatives, and reviewing these alternatives in the light of likely consequences. Gary Klein (1993) notes that managers under stress engage in "recognition-primed decision making." That is, they do not search through long lists of standard operating procedures to determine whether the organization is performing effectively in a given context. Rather, they scan the context in which the organization is operating and check the margins to determine whether observed performance is consistent with their mental model of effective performance. This means that expert personnel are so attuned to their organization and to their usual operating environment that they quickly detect the anomalies, or the points of dysfunction, and focus their scarce time and attention on correcting what is going wrong. In the urgent environment of disaster, time is critical, and identifying the potential threats before they occur is fundamental to avoiding failure and maintaining the operation of the system, even if it suffers some damage. This mode of decision making is consistent with Wildavsky's concept of anticipating risk and taking action to correct potential failures before they escalate to major collapse.

The Edge of Chaos

A third approach derives from the literature of complex adaptive systems. Biologist Stuart Kauffman (1993) regards all systems as operating on a continuum that ranges from order to chaos. Systems operating at the order end of the continuum move toward chaos. Conversely, systems operating at the chaotic end of the continuum move toward order. To Kauffman, there is a narrow band at the center of the continuum in which there is sufficient structure to hold and exchange information but sufficient flexibility to adapt to a changing environment. He terms this area the "edge of chaos," the most creative arena for organizational action. Decision makers who function in this range are likely to be highly innovative in managing scarce resources under urgent time constraints. This model has been observed in disaster field observations (Comfort 1999), most often enacted by a team of experienced disaster managers who not only respect and trust one another but who also complement and correct one another's actions in practice.

The Bowtie Model

A fourth approach builds on the previous models and offers a more systematic approach to managing uncertainty in operational environments. The key function in the previous models is the design of information processes to support learning, while simultaneously updating action strategies to adapt more effectively to a changing environment. Csete & Doyle (2004) combine feedback processes with simultaneity in transmitting information from heterogeneous sources to facilitate coordinated action in complex environments. Termed "bowtie" architecture, the design identifies key sources of data that "fan in" simultaneously to a central processing unit or "knot" where the data are integrated, analyzed, and interpreted

from the perspective and performance of the whole system. This new information is then "fanned out" to the relevant actors or operating units that use the information to make adjustments in their specific operation informed by the global perspective. This design is similar to an Emergency Operations Center, where status reports from multiple agencies are transmitted to the service chiefs who review the data from the perspective of the whole community. The set of service chiefs collectively integrate, analyze, and interpret the data in reference to the performance of the whole response system and then transmit the relevant information to the respective agency personnel, who adjust the performance of their units informed by the operations perspective for the entire system.

This theoretical framework acknowledges the importance of both design and self-organizing action in guiding coordinated action in a complex, dynamic environment. It can be modeled as a set of networks that facilitate the exchange of incoming and outgoing information through a set of analytical activities that support coordinated decision making. The information flow is multi-way, but it gains efficiency through integrated analysis and coordinated action toward a clearly articulated goal for the whole system. It operates by identifying the key sources of information, the key processes of analysis and interpretation for the whole system, and the key routes of transmission. It maintains self-organizing functions in that personnel, with informed knowledge, adjust their own performance to achieve the best performance for the whole system. Design, self-organization, and feedback are central to effective performance of distinct organizational units within the global system.

This theoretical model, using the bowtie architecture, can best be implemented as a socio-technical system. That is, it uses the facilities of an advanced technical information infrastructure to inform the human decision makers who are responsible for maintaining the daily operations of the community. These facilities include the technical capacity to perform the processes of monitoring, integrating, analyzing, and transmitting information regarding community operations in a timely, accurate, and manageable fashion for the human decision makers. The model relies on the human capacity to learn, and it uses the design of a technical infrastructure to facilitate the learning process. Communication of information serves as the driving force for the model and transmits a continuous assessment of the status of the system's vital functions in real time. The performance of the system is measured by the shared commitment to informed action among the participants to achieve the stated goal. The elements of the model are illustrated in Figure 1 below.

Action Models

In each of the four models described above, the objective is to critique actual performance against a prior model of organizational structure in order to improve performance in a continuous process of collective learning. The decision makers use their experience to identify gaps in the organizational system model in order to

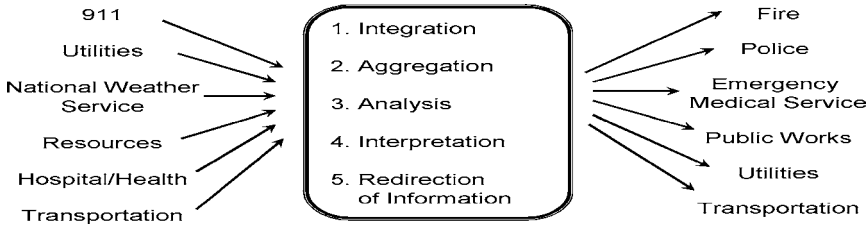

Figure 1 Bowtie model of an emergency operations center.

correct performance for the next event. The logic of these approaches is to identify what the organization does not know in changing environments or new situations and to devise better means of coping with unknown conditions. Acknowledgment of error is not a negative action but rather serves as the basis for learning and contributes to improved future performance. The major resource in each of these models is the capacity of individuals to learn and to transmit that knowledge to other participants in the system. Each approach acknowledges the need to design organizational structures and processes that facilitate individual and organizational learning as well as to identify and correct potential errors on a timely basis. The cumulative effect, seen most clearly in the bowtie model, is to reduce the asymmetry of information, a major cause of dysfunction in complex systems requiring coordination among multiple actors. Yet, the design of learning organizations that can maintain sustainable security but also function effectively in the rapidly changing, urgent environment of disaster requires methods and measurement of performance for dynamic contexts.

MANAGING UNCERTAINTY IN COMPLEX ENVIRONMENTS

The classic response to uncertainty is to recognize the limitations of the existing system and to broaden the scope of actors, agents, and knowledge that can be marshaled for action, as needed. In managing risk, whether from natural, technological, or deliberate disaster, this basic principle of widening the set of resources available to reduce risk applies. Security is a problem not only for government agencies but also for private and nonprofit organizations. Although mitigation and response to natural and technological disasters have historically engaged nonprofit and private organizations as well as public agencies, security has largely been perceived as a function of public agencies. The events of 9/11 demonstrated vividly that maintaining security for a given region requires the collaborative effort of public, private, and nonprofit systems operating along functional lines rather than within jurisdictional boundaries. This perspective is articulated most cogently by

Salamon (Salamon & Elliott 2002) in his discussion of the tools of governance. Salamon & Elliot present a set of financial and organizational instruments for organizing collective action to serve public purposes.

Three concepts are central to implementing a policy for managing uncertainty in complex environments. Each suggests new methods of monitoring and measuring dynamic processes, methods that can contribute to reducing uncertainty in complex environments.

Interoperability of Social and Technical Systems

Interoperability is a term that was initially used in reference to communication systems; it meant the capacity of radio systems operating on different channels to communicate with one another during emergencies (National Governors Association 2002). It also has been used to describe the integration of different formats for technical decision support systems (Walker 2002). The Office of Domestic Preparedness (ODP) defines interoperability as "the ability of two or more public safety agencies to exchange information, when and where it is needed, even when different communication/information systems are involved" (2003, p. 2-1). Although ODP extends the concept of interoperability beyond radios to include fixed facilities, mobile platforms, and portable (personal) devices, its focus is still primarily on communications equipment (Public Safety Wireless Network Program 2002). This focus on communications was broadened in findings from a research workshop sponsored by the U.S. National Science Foundation (Rao 2003). The interdisciplinary researchers and practicing managers who gathered at this workshop recognized the need for interoperability of the highly diverse, large-scale networks of communications and information exchange used by public, private, and nonprofit organizations to provide societal services. The findings acknowledged the centrality of communications to the capacity of different types of organizations to coordinate their actions to manage risk effectively. This same pattern of interactive communication is essential between the operators of technical systems and managers of the organizational systems that use them. Potential failure of interoperability among large technical systems becomes a security threat for the region. Security in large regions of the country, both metropolitan and rural, depends upon the interoperability of different types of technical systems and the organizational systems that manage them. Sustainable security requires functioning electrical power, transportation, communications, gas, water, and sewage distribution systems. These systems are often privately owned, yet serve critical public functions. Managing this technical infrastructure and maintaining its safe operation for public use becomes a key organizational function in developing sustainable security. This task is inherently interdisciplinary and interorganizational, and it explores the interaction between social and technical systems. For example, a report of a failure in a technical system is transmitted to managers of related organizational systems who seek to coordinate response actions and reallocate resources to maintain operations in the larger meta-system that incorporates both.

New models are currently being developed that characterize the operations of these interacting systems (Comfort et al. 2004). One measure represents the demands placed on a technical system, for example, transportation. A second measure represents the response to those demands as messages sent to emergency organizations reporting the technical failure and actions taken by these organizations to correct the failure and maintain the operation of the system. For example, traffic can be modeled on a complex roadway system using cameras and sensors. Should an accident occur and congestion form, information regarding alternate routing or other forms of transportation can be transmitted immediately to support decision-makers in taking constructive action to clear the congestion. Distribution patterns of communication among both technical and social organizations engaged in response operations can be modeled, showing the likely pattern of interaction among the two subsystems as conditions change. This dual dynamic reflects the reciprocal adjustment that each subsystem makes in response to the other, but it also reveals the threshold point of fragility, or the point at which performance in the regional transportation system fails. Such models capture the interaction between risk and resilience (Wildavsky 1988, Comfort 1994), similar to the dynamics in disaster operations.

In these models, information is the primary resource in both technical and organizational subsystems that enables adaptive performance. Consequently, information management, data quality, data currency, and accessibility are requisite for effective management of the larger socio-technical system. Maintaining effective performance requires public investment to create a technical infrastructure that enables scalability of information across the graduated levels of detail needed to support informed action in a complex environment. Scalable information is also essential to enable different audiences with different interests, capabilities, and experience to comprehend a massive event and mobilize common action.

Networks and Computational Simulation

If governance is accepted as a set of interacting networks, traditional methods of monitoring and measuring public performance are inadequate. A related line of research has been developed by sociologists studying the performance of organizations operating in dynamic conditions over time. Kathleen Carley (2000) and her colleagues initially studied how individuals performed under different conditions of resources, information, and time stress (Carley & Prietula 1994, Carley & Lee 1998). In later work, they have extended their analyses to develop computational models of organizational performance under changing conditions (Carley et al. 2001). This method of inquiry offers a systematic means to explore alternative scenarios for organizational action.

A similar approach has also been used to model fragility in disaster response systems (Comfort et al. 2003, 2004), using a theoretical framework of complex systems. Based on discrete dynamics, complexity theory reveals the power of self-organization embedded in complex systems. The interactions among agents who

participate in response operations form a disaster response system that reveals a spontaneous order. Agent-based simulation is used to model those interactions (Carley 2000, 1999) and to study the dynamics of disaster response as a complex system. Although the initial definition of the system focuses on identifying the individual agents and their roles, the scope and order of the system emerges from the interactions among the participating agents. These interactions among the agents define the overall system properties. Both social (Wasserman & Faust 1994) and evolving network theories (Watts 2003, Barabasi 2002) are used to identify the structure of a disaster response network among organizations as well as the core information that is exchanged among the agents. These networks, identified as scale-free, differ from the random networks assumed in earlier social network analysis. That is, the networks are characterized by nodes of dense interaction, with links connecting actors to the nodes, rather than being distributed randomly across a grid of interaction. This pattern of interaction has been termed a small world network, in which it is possible to reach a large number of actors through a very small number of densely connected nodes (Watts 2003, Barabasi 2002). The scale-free networks prove robust under stressful conditions, but are vulnerable if key nodes are disabled. This vulnerability was illustrated by the collapse of telephone communications following the World Trade Center attacks in New York City when the Verizon Communications Center, located under Building 7, was destroyed.

The exploration of networks as an organizational form is particularly relevant to the context of security, which analyzes threats and counter-threats as interacting dynamics. Much of this work has been done by researchers examining threats in battlefield contexts (Alberts et al. 2001). This research uses network analysis and computational simulation as means to identify potential threats, mobilize counter actions, and estimate the potential fragility—or threshold point of failure—for each type of network. The focus is to assess and analyze the characteristics, organizational structures, and dynamics of security threats and counter-threats from the perspective of an interacting, complex system operating on multiple levels in many locations. This approach acknowledges the robustness and fragility of the interacting networks operating within societal and global systems. It focuses on identifying the information structures, mechanisms, evolving knowledge bases, and cultures that serve as resources to both terrorist and counter-terrorist actors/agents. The research investigates the flow of information among the different actors and between their levels of operation as a critical measure of both risk and resilience in an interactive, dynamic process. This approach also acknowledges the importance of learning at individual, organizational, network, and system scales of operation, and uses this process as a major resource in both identifying potential terrorist threats and developing resilient, robust strategies for counter-terrorism. It assumes that the dual dynamics of terrorism and counter-terrorism operate within a global sociotechnical system in which change at one level precipitates change—in vulnerability as well as strength—at other operating levels.

Network analysis and computational simulation offer useful means of exploring different strategies of organizational behavior under changing conditions over time.

These methods enable researchers to test alternative strategies of communication and coordination with other agencies, including potential adversaries. In a world in which threats to security are likely to continue, this approach becomes a necessary part of professional development.

Long-Term Policy Analysis and the Generation of Alternative Scenarios

The problem of uncertainty is particularly acute in efforts to forecast unusual or unstable future strategies. In situations of deep uncertainty, standard methods of analysis based on known data fail. There are too many unknowns to approximate any reliable trends, or to test any potential hypotheses. Addressing the problem of deep uncertainty in a novel way, Lempert et al. (2003) propose an approach to explore potential strategies of action for "the next one hundred years." Their approach is relatively simple. Using computational simulation, they generate a very large number of scenarios for the future, using a range of conditions and patterns of interaction among actors. They do not claim that any one of the scenarios actually predicts the future. Rather, they suggest that a plausible future scenario may be included in the set. They eliminate unlikely scenarios that do not fit the existing context or that practicing decision makers rule out as unworkable. Although no single scenario may be entirely accurate, they suggest that the set of scenarios refined through review and discussion represents a range of situations that could occur. By stretching the imaginations of participating policy makers and analysts, they suggest that this method of exploring the future contributes to the professional development of managers, enabling them to recognize and act on both positive and negative conditions as they emerge.

This method warrants careful consideration, as it is grounded in systematic, rigorous, and detailed analysis of the characteristics and interactions of the actors/agents involved in the selected system. It differs from traditional methods of forecasting in that it considers large ensembles of scenarios; seeks robust, rather than optimal strategies; employs adaptive strategies; and designs analysis for interactive exploration among relevant stakeholders. Its weakness is that it cannot predict which of the potential scenarios is most likely to happen.

In developing potential scenarios, researchers may use a range of research methods for data collection, analysis, modeling, and synthesis of findings. These methods include

- Systematic review and content analysis of documentary reports, case studies, experiments, datasets, and records of terrorist events to characterize the operating agents, structures, modes, and conditions of terrorist and counterterrorist networks.
- Characterization of existing conditions of the networks as baselines for measurement of change.
- Organizational analysis of the interdependencies within and between identified networks, using computational methods.

- Computational modeling of the dynamics of the sets of candidate networks and the interaction between them as well as the thresholds of fragility and resilience within each system.
- Evaluation of the plausibility of the models by practicing managers in public, private, and nonprofit organizations.
- Visual representation of findings to increase effective dissemination to relevant audiences and to increase dialogue, information exchange, and organizational learning among them.

The expected outcomes from this research should enable practicing managers to think about new ways of managing uncertainty and to recognize potential opportunities for constructive action as well as to avoid destructive situations before they occur. This approach seeks to enable practicing policy makers to develop long-term strategies for managing risk that will reduce potential harm to citizens before it occurs.

PUBLIC VALUES IN UNCERTAIN ENVIRONMENTS

In situations of deep uncertainty, rationality is limited. At this point, public values can play a critical role in linking known and unknown conditions within a community. Clearly articulated and cogently presented, public values can serve to bridge the interests and commitments of disparate groups and to support collective action toward a constructive future. The intent is to foster a dialogue that includes all participants in the community. In democratic societies, the function of a continuing dialogue is to identify potential error before it occurs and to make corrections in course as the system adapts to changing conditions. Iris Young (2002) argues that public dialogue is fundamental to democracy, because through dialogue, citizens can explore alternative futures and hold those who exercise public power accountable. Through dialogue, citizens develop the moral authority to act in uncertain conditions.

Recognizing the importance of dialogue to enabling collective action under uncertainty provides a critical lens through which to review the policy actions taken to reduce risk after 9/11. Countering a distinguished tradition of legal protection of privacy through U.S. courts, the U.S.A. Patriot Act enabled government agencies to engage in practices that abridged the norms of individual freedom without warrant or evidence. For example, persons seeking entry to the U.S. could be held in custody without evidence of wrongdoing and without resort to legal counsel (Sec. 213, U.S.A. Patriot Act 2001). Foreign students who were in the U.S. were subjected to new restrictions on travel or renewal of their visas (Sec. 416, U.S.A. Patriot Act 2001). Delays in submitting reports to Congress as a means of monitoring the appropriate execution of intelligence activities were authorized (Sec. 904, U.S.A. Patriot Act 2001). Authority to intercept wire, oral, and electronic communications presumably related to terrorism was broadly granted (Sec. 201, U.S.A. Patriot Act 2001).

Although the rationale for these actions was to increase public security and prevent threats to U.S. citizens, the effect of the U.S.A. Patriot Act often increased fear of privacy violations among citizens (Nelson 2002) and decreased the cooperation essential to sharing information among informed persons that is central to disrupting terrorist networks. Rather than reassuring citizens that enhanced government surveillance activities were being done only for their protection and in limited areas, the jarring experience of government controls placed on citizen activity without requisite evidence appeared to threaten the very freedoms the law was designed to protect.

The question is how to balance security, privacy, and responsible public access to information. Although it provides no certain answers, public dialogue does contribute to the development of intellectual capital within a society. That is, it stimulates among a broad group of citizens a blend of knowledge, professional judgment, trust, and leadership that is critical for innovative action. It supports the development of leaders who have the capacity to articulate a clear vision for the future and to formulate effective strategies for informed action.

FUTURE STRATEGIES

Given the continuing rate of change in a global society in which populations are growing, moving into hazardous areas, and engaging in novel and often questionable behaviors, the risk of natural, technological, and deliberate disasters is certain to increase. As these risks increase, the challenges of anticipating and managing them become more varied and more complex. Strategies of control quickly become outdated and obsolete. Rather, managing risk can best be understood as a continuing process of inquiry, adaptation, and learning.

Three approaches appear most constructive in supporting this task. The first is framing the problem as a continuous process of inquiry, recognizing the complexity and interdependence of risk factors. The theoretical framework of complex adaptive systems supports this formulation and provides an intellectual basis for analysis. The second is the skillful use of computational simulation to generate alternative scenarios for review and discussion of possible futures. Such exercises, based on rigorous characterization of existing conditions, stimulate imaginative exploration of alternative futures. As possible scenarios are reviewed, debated, and considered, they enable citizens to explore innovative strategies and adapt more appropriately to changing conditions. A third approach acknowledges the central role of technology in creating and maintaining sustainable communities and considers the processes of risk reduction, disaster management, and security management as integrated through a socio-technical system.

None of these methods alone can guarantee security, but cumulatively they offer a means of increasing the capacity of communities to manage their own risk. The critical function they perform is reducing the asymmetry of information among different actors and enabling public, private, and nonprofit organizations, as well as households and citizens, to take responsible action to reduce risk. In doing

so, the problem of security is transformed from establishing hierarchical external controls over citizen behavior to enabling informed, timely action by multiple actors/agents in a coordinated effort to anticipate and reduce risk. This approach, building on well-designed information processes, appropriate technical information infrastructure, human capacity for learning, and timely feedback, offers the promise of sustainable management of risk and disaster through harnessing human innovation and adaptation in dynamic environments.

ACKNOWLEDGMENTS

I acknowledge Thomas W. Haase, Esq., for his thoughtful assistance in the preparation of this article, and his careful review of the provisions of the U.S.A. Patriot Act. I also thank Melissa Moran and Lin Huang for their research support.

LITERATURE CITED

9/11 Commission. 2004. *Final Report of the National Commission on Terrorist Attacks Upon the United States*, Official Gov. Ed. http://www.gpoaccess.gov/911/

Alberts DS, Garstka JJ, Hayes RE, Signori DA. 2001. *Understanding Information Age Warfare*. Washington, DC: Dep. Defense Command and Control Res. Program

Barabasi AL. 2002. *Linked: The New Science of Networks*. Cambridge: MA: Perseus. 304 pp.

Carley KM. 1999. On the evolution of social and organizational networks. In *Networks In and Around Organizations*, ed. SB Andrews, D Knoke, 16:3–30. Stamford, CT: JAI Press. 287 pp.

Carley KM. 2000. Organizational adaptation in volatile environments. In *Computational Modeling in Organizational Behavior: The Third Scientific Discipline*, ed. CL Hulin, DR Ilgen, pp. 241–268. Washington, DC: Am. Psychol. Assoc.

Carley KM, Lee JS. 1998. Dynamic organizations: organizational adaptation in a changing environment. In *Advances in Strategic Management*, ed. J Baum, pp. 269–97. Stamford, CT: JAI Press

Carley KM, Lee JS, Krackhardt D. 2001. Destabilizing networks. *Connections* 24(3):31–34

Carley KM, Prietula MJ, eds. 1994. *Computational Organizational Theory*. Hillsdale, NJ: Lawrence Erlbaum Assoc. 318 pp.

Comfort LK, ed. 1988. *Managing Disaster: Strategies and Policy Perspectives*. Durham, NC: Duke Univ. Press. 420 pp.

Comfort LK. 1994. Risk and resilience: inter-organizational learning following the Northridge Earthquake of January 17. *J. Contingencies and Crisis Manag.* 2(3):174–88

Comfort LK. 1999. *Shared Risk: Complex Systems in Seismic Policy*. Amsterdam and Oxford: Pergamon. 322 pp.

Comfort LK. 2003. Managing intergovernmental response to terrorism and other extreme events. *Publius* 32(4):29–49

Comfort LK, Hauskrecht M, Lin JS. 2004. *Dynamic networks: modeling changes in environments exposed to risk*. Presented at the Annu. Res. Conf., Assoc. Pub. Policy and Manag., Atlanta

Comfort LK, Ko K, Zagorecki A. 2003. *Modeling fragility in rapidly evolving disaster response systems*. Work. Pap., Inst. Gov. Stud., Univ. Calif., Berkeley

Comfort LK, Ko K, Zagorecki A. 2004. Coordination in rapidly evolving systems: the role of information. *Am. Behav. Sci.* 48(3): 295–313

Comfort LK, Wisner B, Cutter S, Pulwarty R, Hewitt K, et al. 1999. Reframing disaster policy: the global evolution of vulnerable communities. *Environ. Hazards* 1(1):39–44

Csete M, Doyle J. 2004. Bowties, metabolism, and disease. *Trends Biotech.* 22(9):446–50

Federal Emergency Management Agency. 2000. *Federal Response Plan*. Washington, DC: Fed. Emerg. Manag. Agency

Flin RH. 1996. *Sitting in the Hot Seat: Leaders and Teams for Critical Incident Management*. New York: John Wiley & Sons. 270 pp.

Flin RH, ed. 1997. *Decision Making Under Stress: Emerging Themes and Applications*. Aldershot, Hants, UK: Ashgate. 339 pp.

Kauffman SA. 1993. *The Origins of Order: Self-Organization and Selection in Evolution*. New York: Oxford Univ. Press. 734 pp.

Klein GA. 1993. A recognition primed decision making (RPD) model of rapid decision making. In *Decision Making in Action: Models and Methods*, ed. G Klein, J Orasanu, R Calderwood, CE Zsambok, pp 138–147. Norwood, NJ: Ablex

Lempert RJ, Popper SW, Bankes SC. 2003. *Shaping the Next One Hundred Years: New Methods for Quantitative, Long-Term Policy Analysis*. Santa Monica, CA: Rand. 170 pp.

May PJ. 1985. *Recovering from Catastrophes: Federal Disaster Relief Policy and Politics*. Westport, CT: Greenwood. 186 pp.

May PJ, Williams W. 1986. *Disaster Policy Implementation: Managing Programs Under Shared Governance*. New York: Plenum. 198 pp.

McLoughlin D. 1985. A framework for integrated emergency management. *Public Adm. Rev.* 45:165–72

Mileti D, ed. 1999. *Disasters by Design: A Reassessment of Natural Hazards in the United States*. Washington, DC: Joseph Henry Press. 351 pp.

Nelson L. 2002. Protecting the common good: technology, objectivity, and privacy. *Public Adm. Rev.* 62(4):63–69

National Governors Association. 2002. *Homeland Security: A Governor's Guide to Emergency Management,* Vol. II. Washington, DC: Natl. Gov. Assoc. Center for Best Practices

Office of Domestic Preparedness. 2002. *Developing Multi-Agency Interoperability Communication Systems: User's Handbook*. Washington, DC: Dep. of Homeland Secur.

Platt R. 1999. *Disasters and Democracy*. Washington, DC: Island Press. 320 pp.

Posner PL. 2002. *Homeland Security: Effective Intergovernmental Coordination is Key to Success*, GAO-02-1013T. Washington, DC: Gen. Account. Off.

Public Safety Wireless Network Program. 2002. *Fire and EMS Communications Interoperability*, Information Brief. Washington, DC: Dep. Justice and Dep. Treas.

Rao R. 2003. *Cyberinfrastructure research for homeland security*. Natl. Sci. Found. Workshop Rep. University of California, San Diego

Rochlin GI. 1993. Defining high-reliability organizations in practice: a taxonomic prologue. In *New Challenges to Understanding Organizations*, ed. KH Roberts, 2:11–32. New York: Macmillan. 256 pp.

Salamon LA, Elliott OV, eds. 2002. *The Tools of Government: A Guide to the New Governance*. Oxford: Oxford Univ. Press. 669 pp.

United States Government. 2001. *United States Government Interagency Domestic Terrorism Concept of Operations Plan*. http://www.fbi.gov/publications/conplan/conplan.pdf.

U.S.A. Patriot Act. 2001. *Public Law 107–56*. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

Walker D. 2002. *Homeland Security: Critical Design and Implementation Issues*. Testimony before the Select Committee on Homeland Security, US House of Representatives, July 17, 2002, GAO-02-957T. Washington, DC: Gen. Account. Off.

Wasserman S, Faust K. 1994. *Social Network*

Analysis: Methods and Applications. Cambridge: Cambridge Univ. Press. 857 pp.
Watts DJ. 2003. *Six Degrees: The Science of a Connected Age*. New York: W.W. Norton. 368 pp.
Weick KE. 1995. *Sense Making in Organizations*. Thousand Oaks, CA: Sage. 235 pp.
Weick KE, Roberts K. 1993. Collective mind and organizational reliability: the case of flight operations on an aircraft carrier deck. *Admin. Sci. Q.* 38:357–81
Wildavsky AB. 1988. *Searching for Safety*. New Brunswick, NJ: Transaction Books. 253 pp.
Young IM. 2002. *Inclusion and Democracy*. Oxford: Oxford Univ. Press. 528 pp.

Annual Review of Political Science
Volume 8, 2005

CONTENTS