10

ORGANIZATIONAL STRATEGIES FOR COMPLEX SYSTEM RESILIENCE, RELIABILITY, AND ADAPTATION

Todd M. La Porte

With thousands of miles of unprotected borders, tens of thousands of critical power generating plants, chemical processing units and other hazardous manufacturing facilities, and hundreds of thousands of miles unprotected roads and rail, electric, gas, and telecommunications lines, the United States is impossible to protect completely against terrorist attack. In addition to military action against terrorists abroad and use of intelligence to intercept attacks before they are launched, what organizational strategies are best suited for providing homeland security and protecting critical infrastructure? In this chapter, I address the problem of critical infrastructure protection from an organization studies perspective. I begin by discussing the nature of critical infrastructures as large technical systems with distinct organizational properties. I then turn to organizational strategies to deal with what is identified as a "wicked" problem. While no specific organizational solution will solve critical infrastructure protection, a number of strategies may help solve it, notably the encouragement and protection of high reliability organizations and professionals who work in them. Finally, I argue that political leadership will be necessary to effect the changes proposed.

THE NATURE OF CRITICAL INFRASTRUCTURES

Critical infrastructures exhibit characteristics of large technical systems.[1] Their technology and organization are highly complex. Key elements are geographically dispersed, but they are linked together in networks and nodes, with varying degrees of connectivity. Some systems, such as telecommunications and electric power, operate in real-time (meaning that there is no possibility of stockpiling or scheduling demand – the whole system, from end to end, is "on"

all the time). Other systems are less subject to the requirements of real-time operations, but even short or unexpected interruptions, for example in local road or container cargo traffic, can cause major economic and social disruption. The disruptions caused by Hurricanes Katrina and Rita on oil wells and refineries in the Gulf Coast region are cases in point.

As examined in more detail in Part IV of this book, most critical infrastructures are highly interdependent: telecommunications and electric power systems require each other to function, and both support the operations of almost every other element of infrastructure, including the Internet. Water distribution depends to a great extent on electric power for pumping and water treatment. Road traffic would quickly snarl if control systems were without electricity and telecommunications. Electric power generation would be compromised by disruptions in pipeline, rail, or truck transportation.

Large technical system organization is tightly coupled as well, which for normal operations improves efficiency. However, it is increasingly recognized that tight coupling can also lead to increased vulnerability to disruption, prompting many organization managers to adopt defensive management practices, stockpiling, and extensive relationship-building with outside organizations, which can reduce the very efficiency tight coupling is intended to increase.

Sociologist Charles Perrow argues that failure is inherent in complex tightly coupled systems: the centralization of decision-making authority required to manage tight coupling conflicts with the decentralization of authority required to deal with unanticipated problems by those closest to them throughout the organization.[2] Operators of complex tightly coupled systems need, but generally cannot have, both centralization and decentralization to make sure that such systems do not fail across a wide variety of operating conditions.

These management requirements are different from those of loosely coupled systems, such as most manufacturing, mining, office work, and lab research, where authority can be either centralized or decentralized, as the task dictates. The management requirements of tightly coupled but linear systems, such as continuous process industries, most transportation, and regulated electric power, are also different: authority by operators can be centralized because the information needed is easily provided and acted upon.

Technological change in and of itself may be a source of disruption to large complex systems, or at least it may establish conditions that make disruptions easier to achieve. New technologies require new organizational structures and processes and often demand that employees acquire new skills and ways of working.[3] When change is very rapid, the gap between the new technological capabilities and the capacity to regulate, monitor, or mediate the effects of these technologies may be wide enough that economic or social problems arise.

The history of most important technologies demonstrates this. It took some years, and many accidents, after automobiles were introduced for traffic regulation systems to be instituted. The electricity crisis in California in 2000 and the August 14, 2003, blackout in the United States and Canada both show how technological change, in these cases arising from deregulation, make system stability more problematic. The lag between a technical system's new operating conditions and the economic, regulatory, and social frameworks that shape and moderate the effects of the newly "liberated" technologies, means that unintended negative consequences may accompany the intended positive ones.

THREATS TO CRITICAL INFRASTRUCTURE PROTECTION

Different types of potential disruptions demand different types of organizational responses, some of which contradict others. Relatively well-understood and regular sources of disruption, such as hurricanes or other severe weather, permit routinized responses. These responses often include well-structured organizations, relatively predictable budget requirements, building codes to reduce vulnerability, and standardized emergency preparedness procedures.

On the other hand, terrorism exhibits high variability and dynamic uncertainty.[4] The unpredictability of the threat demands that organizations become more internally complex, engage in more interaction with outsiders, become more flexible in their organizational structures, and become more adaptive to a wide range of possible contingencies. In terrorism, purposive actors or predators may seek vulnerabilities in complex systems and try to exploit them for maximum disruptive effect. Terrorists understand that disrupting infrastructures multiplies damage throughout society, signals that public authorities are powerless to stop attackers from pursing their political objectives, and limits the ability of the government to provide for its own citizens.

Attacks involving chemical, biological, or nuclear weapons pose the possibility of far greater damage to life and property than is likely to be achieved by conventional weapons. Preliminary data suggest that chemical, biological, and nuclear attacks may be increasing in frequency, but they are still rare and difficult to carry out.[5] Creating a highly effective weapon of mass destruction from toxic chemicals, infectious diseases, or fissionable nuclear material – a process called "weaponization" – is more difficult than many believe. Nevertheless, security authorities are concerned that the technologies of weaponization will spread as familiarity with the technologies increases, particularly with the availability of freelance unemployed former Soviet and South African weapons scientists, and as costs of biotech equipment and supplies continue to decline.[6]

Terrorist attacks are serious challenges for many organizations that have previously faced stable environments and no predators, as well as for organizations that face regular or predictable extreme events, such as hurricanes. Both types of organizations may be called on to deal with both routine and nonroutine types of events, but for them to do so will entail the ability to operate in both modes interchangeably. More importantly, multiple-mode readiness will require that organizations maintain multiple operational capabilities, and that they protect those capabilities in often difficult budgetary and political circumstances. Emergency management and preparedness organizations find it difficult to sustain public and policy attention to their needs once a disaster has passed.

As early as 1976, sociologist Barry Turner studied disasters to find out why many organizations fail to heed what in retrospect were signs of impending disaster.[7] He found that the conditions under which large-scale intelligence failures result include: rigid institutional beliefs, disregard of outside complaints, difficulty handling multiple sources of information, and the tendency to minimize danger. These elements incubate until they become part of the organizational culture, setting the stage for a serious problem to be triggered by an event that in other circumstances might be easily dealt with.

Turner argues that organizations perform poorly when faced with ill-structured problems, which they generally attempt to address by simplifying reality, falling back on habit or ritual, or resorting to rules of thumb. Some organizations attempt to deal with uncertainty by identifying goals and developing plans to achieve them, but in contingent and complex situations they have a hard time knowing whether they have done enough. Thus, organizations that fail to take steps to develop flexible, complexity-embracing and problem-seeking capabilities – and fail to develop organizational cultures that learn from their environments – are likely to experience a disaster in one form or another.[8]

Such observations have important implications for public safety and homeland security organizations. Emergency management and fire and police forces each have a clear mission and have operated in stable task environments, and they have largely been ability to manage most contingencies successfully. Changes have come, to be sure: over the last several decades, the "all hazards" approach to dealing with disasters has supplanted the segmented approach to emergency management and public safety, resulting in increased attention to cross-training and coordination among different emergency response units.

Terrorism, however, poses fundamental challenges to first responders and public safety practices. One wonders how effective any U.S. public safety organization can be in the face of suicide bombers or biological attacks, for example, neither of which have been used widely, if at all, in the United States. Even countries such as Israel, where suicide bomb attacks occur regularly, have great

difficulty in combating the problem and reorganizing both organization structures and practices to attempt to keep on top of it.

Given the difficulties facing public safety organizations, it should be no surprise that serious challenges are also facing the operators of large technical systems. In the United States, these systems are mostly held in private ownership, and their public regulators are mostly unfamiliar with day-to-day operations. Firms and their regulators each have a history of operating in a safe domestic environment, often as regulated monopolies, with linear and less tightly coupled systems and, until more recently, have operated with relatively low levels of system interdependency.[9]

Today, however, with greater interdependency, more exposure to market forces, greater geographic dispersion, and, in some cases, more components that are unique and difficult to replace (as is the case with aging transformers in electric power distribution), large technical systems are more difficult than ever to manage successfully.[10] In addition, many of these infrastructures have themselves become more complex, through new developments in technology and/or as they face newly deregulated markets. Even without the added threat of terrorism, these systems are facing unprecedented stress, increased operating volatility, and occasionally costly system failures.[11]

RESPONSE STRATEGIES

Despite advances in risk assessment methods and improvements in the government's ability to manage disaster response successfully, extreme events – particularly technological or industrial disasters – appear to be increasing in frequency and severity. Terrorist attacks, while historically insignificant sources of harm to the United States, are increasingly worrisome because of their unpredictability in type, scale, and timing. Industrial accidents and terrorist attacks may be characterized by indeterminate but potentially catastrophic damage over large areas, poor and/or rapidly changing situational information, lack of precedent on which to base problem assessment and response, unfolding of events in real time, and active mass media coverage worldwide.[12] This combination could be termed a "wicked problem" of crisis management and critical infrastructure protection. [13]

Rittel and Weber coined this term to describe a class of problems for which there is no definitive problem formulation, for which it is difficult to tell when the problem is solved, – that is, there is no "stopping rule" – and for which there are no unambiguous solution criteria, or in fact any well-described set of possible solutions, because such problems are essentially unique. Wicked problems are often symptoms of other wicked problems, because they often interlock, change over time and depend highly on specific contexts. In fact,

different stakeholders will describe the same wicked problem in quite different ways. What is more, in working on these problems, analysts do not have the luxury of failing, or of learning by trial and error. Examples of wicked problems include thorny value-laden issues such as siting of toxic waste facilities, dealing with environmental problems, reforming social security systems, and establishing fair taxation schemes. Ordinary problem-solving techniques cannot yield unambiguous or widely accepted solutions.

The implications of wicked problems for critical infrastructure protection are serious. Their wickedness implies that solutions that aim to maintain current ways of life without any change may not be possible, or if possible, may not be beneficial. The inherent openness of the United States, both culturally and geographically, limits the ability of any strategy of "hardening" to be completely effective. As government officials often assert, the nation's defenders have to be successful *all* the time, whereas terrorists only have to be successful once. While the homeland security initiatives undertaken by the government are mostly prudent, worthwhile, and uncontroversial, they will not completely protect the nation from another serious terrorist attack. Therefore, it is worth exploring additional strategies to anticipate, adapt to, or respond to attacks or extreme events. These may be divided in three major groups:

- *Macro strategies* – strategies implemented by the government to address external threats: border control, asset hardening, protection, and coordination of emergency response
- *Micro strategies* – strategies implemented by specific organizations to limit vulnerability to disruption or to prevent predators from using organization as launching pads for attacks: vulnerability assessments, contingency and continuity of operations planning
- *Structural strategies* – strategies implemented by government together with key private or non-governmental organizations to deal with industry operations on a sector-wide or intersystem basis

Macro strategies are the essence of what the federal government has undertaken in the months following September 11, 2001. Asset identification and protection is at the heart of critical infrastructure protection as defined by the Office of Homeland Security and later the Department of Homeland Security. Strengthening emergency response capabilities by improving first responder coordination across various governmental and territorial jurisdictions is another type of macro strategy.

Micro strategies are essentially what public and private businesses and organizations do in conducting infrastructure vulnerability assessments. Contingency planning, business continuity planning, and incident management are all terms to describe the analysis of business processes with a specific focus on

minimizing obvious weaknesses that predators could use to disrupt operations or launch further attacks. Perimeter and facilities access control, employee background checks, co-location of utilities, siting of key facilities and the like make up the core elements of these micro strategies of critical infrastructure protection. These measures are less often the subject of governmental policy and more often the result of prudent operations management and planning.

Macro and micro strategies are reasonably well understood as matters of policy, as the recent series of homeland security presidential directives indicate. Implementation may be difficult, as long-standing federal–state relationships are challenged, and as standard operating procedures, budgets, oversight, and accounting are pressured to reorganize. Nevertheless, these strategies are likely to improve the capacity of the nation to deal more effectively with extreme events or terrorist attacks.

Structural strategies are less well developed in critical infrastructure and homeland security policies. Such strategies focus largely on organizations and their relationships with one another, where organizations are considered as purposive actors in their own right. This perspective is also concerned in part with the interaction of public policy with private business: whether or not 85 percent of all infrastructure is owned and operated by the private sector, as is often claimed,[14] it *is* true that infrastructure operators have more extensive relationships with federal, state, and local public and regulatory authorities than do other types of private enterprises. Thus, an important component of an overall critical infrastructure protection policy requires attention to structural and organizational strategies.

ORGANIZATION STUDIES AND CRITICAL INFRASTRUCTURE PROTECTION

From an organization studies point of view, what strategies might be appropriate for organizing long-term critical infrastructure protection? Several approaches can help answer this question: anticipation and resilience, organizing for high reliability operations, and reframing the question to permit consideration of more fundamental alternatives.

ANTICIPATION AND RESILIENCE

Because societies depend on a wide range of infrastructures and services, preventing their disruption and restoring their functioning become important policy concerns. But prevention and restoration are two end points in a continuum that also includes middle-range concerns: assuring organizational or system robustness (the ability to fail gracefully rather than catastrophically)

and organizational or system resilience (the ability to recover quickly once a disruption has occurred).

Political scientist Aaron Wildavsky proposes that strategies of anticipation work best against known problems, whereas strategies of resilience work best against unknown ones.[15] Anticipatory strategies can immobilize much wasteful investment against threats that may never materialize, whereas resilience strategies involve the potential for small or short-term sacrifice in the interest of long-term survival. Furthermore, an over-reliance on anticipation can lead to loss of capacity of an organization to adapt to changing conditions or threats, which can lead to even more vulnerability in the future. As Wildavsky writes, "grass bends before wind but usually does not break; it is temporarily unstable. Trees maintain strong stability under high winds but when they break, they have no resilience. The damage is irreversible, even after the wind has died down."[16]

Wildavsky argues that each strategy is appropriate to specific conditions. When uncertainties are large, resilience is probably the most appropriate. When conditions are stable, and when projections about the future are generally correct, anticipation works best, although it should be used judiciously, as hazards come in many shapes and sizes, and the future is inherently difficult to predict. Strategies of anticipation require exclusively dedicating resources in specific or concrete ways, so there is always the risk that an anticipatory strategy will end up being costly in the long run. As Wildavsky says, "real human situations usually involve a mixture of the known and unknown; hence, there is a tradeoff – the most likely large dangers, if they are known and can be countered without making things worse, can, and should be, prevented."[17]

Resilient systems and organizations are those that rapidly acquire information about their environments, quickly adapt their behaviors and structures to changing circumstances, communicate easily and thoroughly with others, and broadly mobilize networks of expertise and material support.

An approach that emphasizes resilience is compelling for many types of hazards, though adopting it may be more feasible in the long rather than short-term. Accepting mass casualties from a terrorist attack would be unacceptable for most societies, and most would choose a strategy of anticipation to prevent one from occurring. Yet anticipation against the dynamic uncertainty of terrorism has its drawbacks as well. Organizations facing low probability but high cost consequences and dynamic uncertainty confront contradictory imperatives that can produce a schizophrenic response, or worse, organizational paralysis.

HIGH RELIABILITY ORGANIZATIONS

Most large organizations exhibit such characteristics as highly formalized structure, long-standing operating procedures, lack of adaptability in the face of new

problems or changes to their environments, and the like. Small organizations are less rigidly structured, engage in more ad hoc business processes, and are generally more adaptable to change, but they are also generally less complex and cannot sustain stressful operations for long without collapsing.

Resilience as a strategy for typical organizations is appropriate when trial-and-error learning is acceptable and when the cost of errors is low. But when the potential or expected cost of error is high, successful organizations tend to assume behaviors of high reliability or mindful organizations.[18]

This unusual class of organizations addresses the apparent contradiction between anticipation and resilience. Organizations such as nuclear power plants, air traffic control centers, and certain types of military operations have come to perform nearly flawlessly even under the most stressful of conditions. Yet these operations are also extraordinarily complex, operate hazardous processes, function within very tight time constraints, and are technically or organizationally tightly coupled, either among subsystems or with outside systems.

In addition, these organizations are able to shift seamlessly from routine operating modes, where formal organizational attributes such as hierarchical authority and standard operating procedures dominate organizational activities, to "high tempo" activities, where more informal organization norms dominate. During high tempo periods, operating experts are given great latitude to control operations, communication flows where needed (unhindered by the chain of command), and the problem is the focus of everyone's activities, regardless of their formal position in the organization.[19] These organizations' ability to function well in times of normalcy and chaos defies conventional understandings of how large complex organizations operate.

The ability to switch between two modes of operations – one emphasizing planning and routines, and the other focusing on contingency and rapid response and adaptation – appears to reconcile the competing requirements of both anticipation and resilience in highly reliable organizations. These properties also characterize much of the most demanding activities involved in critical infrastructure operations, particularly if they are attacked or must operate under unusually stressful conditions. These overall properties of highly reliable organizations should make them extremely attractive to critical infrastructure operations, and in fact a number of them independently possess these characteristics.

In addition to being able to switch easily between normal and crisis modes, highly reliable organizations essentially perform with high levels of technical competence over long periods. One way they do this is to reward error discovery and correction. They are occupied with failure, something regular organizations often do focus on. In addition, they avoid simplifying information about environment or tasks, also an unusual characteristic (as noted earlier by Turner

in the previous passage). Authority systems inside the organization are unique as well, in that they often have redundant operational and supervisory systems that are relatively collegial and decentralized. People with technical expertise, regardless of status or rank, are given great deference in making decisions, and they receive intensive and regular training. No matter the economic fortunes of the organization, training is simply not negotiable. Finally, highly reliable organizations share information openly with external overseers, regulators, and the public, but they also protect their sensitive operations from external interference at nearly any cost.[20]

It is important to note that an organization cannot calibrate its degree of reliability by choosing some features and leaving others aside, perhaps as too costly or inconvenient. These attributes evolve in organizations tasked with extraordinarily demanding functions where funding is generous and the mission supported by key external overseers. They are difficult to maintain without constant attention and overall institutional stability. They cannot be transferred into organizations from outside, as they are tightly knit into the fabric of organizational culture and the specificities of the work process. If the conditions that have given rise to these organizations change, their continued ability to perform so reliably cannot be assured.

RELIABILITY PROFESSIONALS

A common thread in resilient and reliable organizations is active and engaged management by highly trained professionals. Compared with automated systems, human professionals in sensitive decision-making positions have far greater ability to adapt quickly in these complex systems. Automated systems cannot acquire information outside the parameters the system designers envisaged, and they cannot develop novel problem-solving routines on the fly.[21] An often-noted characteristic of key operators in such systems as air traffic control and electric grid operations is that they "have the bubble." This state of hyper-awareness is critical to successful high-tempo operations.[22] Therefore, processes that depend on automated decision support have difficulty coping either with extreme complexity arising from system behavior or with dynamic uncertainty created by adversaries who learn.

Schulman and Roe, in this book (Chapter 9) and in previous work, emphasize even more strongly the importance of what they term *reliability professionals* in sustaining the effective functioning of critical functions in large technical systems.[23] They argue that essential but largely unrecognized staff members of critical infrastructure system organizations are vital to the task of "keeping the lights on" in the face of extraordinary system volatility or stress. These professionals cycle between their on-the-job knowledge of how large-scale systems

typically function and their ability to understand the systems' overall macro-design. In this sense, they embody characteristics analogous to those of high reliability organizations.

Schulman and Roe (Chapter 9) and their colleagues argue that reliability professionals both look at the detailed day-to-day problems they face and develop sophisticated pattern recognition capabilities, where they use trial and error learning to develop their deep and often tacit knowledge of the system they are operating. They know the formal attributes of the designed system in which they work, but they are required as a condition of keeping the system running to depart from these design principles and develop contingency scenarios or workarounds to compensate for shortcomings in the original design. This dual cognitive/operational activity enables these staff members to keep systems from failing, even in the face of a wide variety of contingencies. They are thus essential elements of an overall strategy for maintaining system reliability.

In addition, the existence of organizational slack – in terms of resources, control, and conceptual understanding of the system and its environment – permits organization managers to hedge against surprise and to exercise the authority they need to manage the unexpected.[24] While slack has negative connotations for many, depletion of slack in many critical systems limits the ability of managers to run them successfully. This is all the more alarming because many of these systems control powerful and hazardous technologies vital to society.

SYSTEMS OF SYSTEMS

As society increases its reliance on critical systems, maintaining conditions for high reliability operation of larger systems of systems will be essential. It is already demanding enough for single organizations to carry out these requirements. Sustaining reliability across large systems of organizations will require extraordinary effort, both by operators of technical systems and the regulatory and political authorities that oversee them. Yet economic pressure to improve efficiency by utilizing complex and interdependent systems is difficult to resist, despite evidence that such a strategy also entails increasing vulnerability to disruption and makes these systems more attractive targets for terrorism or any sort of sabotage.

Competitive pressures in market environments also require organizations to deploy all resources, both physical and human, at or close to the margin. This increases pressure on line managers to reduce organizational slack to a minimum. Where challenges can be predicted, where warnings are timely, or where the threats are not fatal, organizations can afford to operate close to the margin, because they can react before disaster strikes.

But under conditions of competition associated with deregulation, many large-scale technical systems do not exhibit the same degree of inherent robustness that normal competitive organizations have. For large technical systems, competition leads to eliminating redundancies, cutting excessive staff, paring down non-essential programs such as training, and operating close to margins to achieve short-term economic objectives. Pains have been taken to construct market rules for formerly regulated services (e.g., electricity and telecommunications), but these have had mixed results, as demonstrated by the August 14 blackout of 2003 and the California energy crisis of 2000.[25] For other technical systems such as NASA's space shuttle program, time and economic pressures led to similar corner-cutting, with the well-known disastrous results.

For large technical network systems, increasing interdependence among many organizations intensifies the problem of assuring failure-free operations. For example, the tension between organizational autonomy and independence of the constituent units of the large-scale system makes communication among elements critical. As discussed in more details in Part IV of the book, managers face great difficulty knowing what remote units are doing, which makes decision making problematic because an action in one unit may have unintended consequences elsewhere in the system. Systems of interdependent organizations or complexes are only as reliable as their least reliable part. Risk migrates to these weak links, unknown to other system operators.[26]

Providing sufficient slack, encouraging constant and clear communications, and creating a consistent belief structure and safety-embracing culture help reduce the problem but cannot eliminate it entirely. Risk migration may be limited by ensuring that large-scale systems have a variety of organizational structures, but these structures need to be flexible in adapting to rapidly changing situations if crises or breakdowns are to be avoided.[27]

In addition, there is considerable concern about "cascading failures" among tightly interdependent infrastructure systems.[28] This concern has provoked a number of efforts to understand the technical and operational dimensions of interdependence through modeling and simulation.[29] Although the technical community strives to understand the causes of cascading failures and to design and build systems that will resist them, it is unclear whether technical solutions can ever permanently prevent large-scale outages.[30]

MULTI-ORGANIZATIONAL COORDINATION

How can one improve resilience in a context of large system interdependence? Critical infrastructure protection will not be secured by a single organization. Rather, it will be the outcome of many organizations working together in concerted fashion. However, it is a common problem in public administration

that the coordination and cooperation needed for effective performance is nearly always lacking. As Pressman and Wildavsky put it in their classic text on implementation, "no phrase expresses as frequent a complaint about the federal bureaucracy as does 'lack of coordination.' No suggestion for reform is more common than 'what we need is more coordination.' "[31]

Guy Peters, a respected scholar of public administration, adds that "the fundamental problems of coordination have been exacerbated by the growth and structural elaboration of modern governments, but the coordination problem appears endemic to all large organizations, or collections of organizations, whether public or private."[32]

These conclusions are reinforced by recent experience in critical infrastructure protection and homeland security. The decision by Congress to create the Department of Homeland Security from 22 separate agencies in a number of federal departments was a response to the coordination issue: supporters of the decision believed that by putting all the relevant parts under one institutional umbrella, better coordination and control of the issue could be achieved. Observations by many close to the department indicate otherwise, however, and some worry that if the department does not clarifying its goals and rethink its structure and priorities, the United States will continue to remain vulnerable to attack.[33]

Although these claims of continued vulnerability may be exaggerated, it certainly will take some time for the new department to forge the cooperative ties among constituent bureaus, and among outside organizations with a stake in its work.[34] This is all the more pressing a concern given the multi-dimensional and dynamic nature of the problem, the requirements for extremely high standards of performance, and the complex and politically charged environment in which the relevant agencies operate.

Peters argues that lack of coordination arises from different operational responsibilities and legal requirements that place significant barriers between organizations, and that this is as much a policy issue as it is one of implementation or execution. Government reform efforts that include privatization and competition make the problem of coordination even more difficult. Three classic organizational responses are possible – hierarchies, markets, and networks. Hierarchies can solve coordination problems by fiat, and they may reduce transaction costs among organization subunits. But hierarchies generally require such a large degree of centralization of information that they restrict the degree of autonomy of "lowerarchs" to act as circumstances dictate. Markets require means of exchange and lots of participants to be effective in coordinating a large number of individuals and organizations. These conditions, however, may violate the spirit or even the letter of the law in cases involving coordination in multi-organizational systems, particularly those dealing with specific actions

for public safety. Networks can effectively coordinate policy and operations (and professional networks can be especially useful in multi-organizational systems), but they work by bargaining among network participants and lack accountability or the ability to direct certain action. Furthermore, people and organizations can be part of multiple networks, so it may be difficult to discern conflicts of interest.[35]

Peters concludes that reform of governmental structures is not enough to improve coordination. Active and sustained intervention by political leaders will be necessary to achieve lasting results.

COMPLEX ADAPTIVE SYSTEMS

A final organizational strategy potentially useful for critical infrastructure protection comes from scholars of complex adaptive systems. Kauffman observed that some biological systems appear to organize themselves at the "edge of chaos," that is, there is enough order for information to be exchanged and stored, but there is sufficient flexibility of structure or procedure to adapt quickly to rapidly changing external situations.[36] Comfort examines a number of disasters to which she applies the "edge of chaos" idea and derives four conditions for effective, adaptive response: (1) articulation of commonly understood meanings or understanding of the threat between a system and its members; (2) sufficient trust among leaders, organizations, and citizens to overcome uncertainty and enable members to accept direction; (3) sufficient resonance or support of the community between the emerging system and its environment to gain support for action; and (4) sufficient resources to sustain collective action under varying conditions.[37]

These conditions can be measured technically, organizationally, and culturally. Technical measures include the state of the infrastructures used by the system to respond to disasters, such as communications or transportation. Organizational measures pertain to the degree of organizational adaptability to new and changing situations, style of communications among system participants, and character of leadership. Cultural measures include willingness to accept new ideas or new types of action. Comfort argues that variations in each of these characterize different degrees of system adaptability, as shown in Table 10.1.

Comfort argues that the overall homeland security system response to the attacks on September 11, 2001, was that of an "operative-adaptive" system. Moving to an "auto-adaptive" system (the most desirable state) will take concerted effort. She suggests three broad policy directions to improve governmental response to such attacks and to reduce future threats. First, organization leaders should improve complex inter-organizational system performance by

Table 10.1. Stages toward adaptive responses

System type	Technical	Organizational	Cultural	Characteristics
Non-adaptive	Low	Low	Low	System operates only with outside assistance during crisis, returns quickly to non-adaptive state
Emergent adaptive	Low	Medium	Medium	System develops way of responding during crisis, but cannot sustain collective response once threat has passed
Operative adaptive	Medium	Medium	Medium	System functions well during crisis, but cannot sustain new responses and threat reduction
Auto-adaptive	High	High	High	System functions effectively in response to varying threats, continues to develop new means of learning and acting

Source: Developed from Comfort 2002.

studying past failures, with particular attention to communication and coordination problems in multi-jurisdictional settings. Second, leaders need to recognize that emergency operations are inherently non-linear and dynamic, and they are not manageable by traditional rational and linear methods. Willingness to permit dynamic rescaling of response will result in more creative and effective operations against unpredictable threats. And third, leaders should facilitate the transition to continuous organizational learning by making substantial investments in information technology and organizational reforms to take advantage of new information technology-enabled capabilities.

POLICY APPROACHES FOR CRITICAL INFRASTRUCTURE PROTECTION

Critical infrastructure protection in the context of anti-terrorism is fraught with difficulties arising from the dynamic uncertainty of the threat, the organizational demands for reliability of infrastructure systems, the problems associated with multi-organizational coordination, and the challenge of achieving

continuous organizational learning in these conditions. What is more, the infrastructures must respond to these difficulties while also remaining competitive in the long run.

Individually, each one of these is an extraordinarily difficult problem. In the context of critical infrastructure protection, the difficulty of addressing them together justifies our earlier characterization of them as "wicked." The problem of terrorist attacks, like other extreme events or disasters, is not one that can be definitively solved, despite presidential campaign rhetoric to the contrary. But progress can be made.

In addition to the obvious macro and micro strategies of infrastructure protection, infrastructure vulnerability assessments, and continuity of operations planning, there is a set of related structural and organizational strategies that should be considered to improve the capacity of the nation's critical infrastructure service providers and public authorities to perform their functions. I conclude this chapter by highlighting six of them.

First, organization leaders should seek to strike a balance between strategies that emphasize anticipation with those that emphasize resilience. The critical infrastructure protection debate has quickly moved toward anticipation and the accompanying efforts to prevent entry of hostile actors, to identify and harden assets, to simulate and then eliminate or protect system vulnerabilities, and so on. This may be the right solution, but given the nature of the large technical systems with which we live, an externally oriented approach that emphasizes hardening is likely to be economically and politically costly. Should it fail once, consequences could be catastrophic.

Therefore, strategies that emphasize resilience – by keeping critical infrastructure protection activities constantly engaged in improvement and learning – should be explored, both because they are likely to be less costly and because they are likely to increase success against actors trying to use dynamic uncertainty to their advantage. Resilience cannot be the only strategy; a catastrophic attack on a major city such as New York, Tokyo, or London might be so costly that protection would be worth the economic and political expense.

Second, strategies that recognize the importance of high-reliability organizations and auto-adaptive systems are essential. These organizations and systems may help point the way to addressing the operational problem of low frequency, high consequence events. Sustaining attention or watchfulness over long periods of time and getting the proper response at the right time will require an extraordinary organizational effort. High-reliability organizations appear to be better equipped than most to do so. Buttressing them with overall systems that promote continuous organizational learning, even in the face of long periods of threat quiescence, are necessary to deal with the twin problems of low frequency and terrorist attackers.

However, the literature on highly reliable organizations does not cover the way in which organizations come to possess their special characteristics, or what managers have done, not to mention what they should do, to steer their organizations in this direction. Researchers in this field assert that identification of the characteristics of highly reliable organizations is not the same thing as knowing how to make them so. More research is needed to learn how such organizations evolve and what can be done to stimulate their development to suit new homeland and national security purposes.

Third, strategies that promote and protect the professionalization of reliability are needed. It should be recognized that people make organizations work, particularly in the demanding domain of critical infrastructure. Minimizing the conditions that disrupt or impede the work of reliability professionals is essential to their ability to maintain the edge they need to keep the lights on and vital systems running. This means taking a close look at the policies that affect major systems, such as deregulation, and asking, "how will these changes affect reliability?" rather than only "how will they affect efficiency?" There appears to be an imperfect market for reliability, and this imperfection demands attention by public authorities to ensure it is provided at the highest possible level.

Fourth, risk will migrate over time to the weakest element in systems of organizations without operators knowing it or being able to manage it. These systems characterize increasing portions of our economy and society, making the migration of risk especially troubling. Policies will need to focus attention on the problem, reward sharing of information about technical and organization changes, encourage strong safety cultures, and protect against the consumption of slack.

Fifth, the classic approaches to taming wicked problems should be pursued: extensive dialogue should take place, by various means, among citizens and stakeholders about the meaning of critical infrastructure protection and homeland security, and the consequences of proposed security solutions. Rittel and Webber argue for "an argumentative process in the course of which an image of the problem and of the solution emerges gradually among the participants, as a product of incessant judgment, subjected to critical argument."[38] It is only through such processes of deliberation, critique and interpretation that problem re-formulation or re-framing can occur, which can ultimately lead to acceptance of problems as less wicked, more amenable to conventional problem solving, and more legitimate.

Finally, political leadership is essential for sustaining the appropriate degree of attentiveness to the problem of coordination across many organizations. Reform fixes may help improve the ability of many agencies to work closely with one another, but in and of themselves will not do the trick. Classically,

reform efforts typically occur in the immediate aftermath of a disaster when public attention and political will is high. As time passes, attention and concern wane, unless reinforced by additional catastrophes. As the record shows, sustaining watchfulness and the ability to anticipate and deal with low-probability high-impact events is the single most difficult policy issue facing emergency management and homeland security.

No single answer will solve critical infrastructure protection. This multifaceted problem requires a variety of responses. A perspective that recognizes the large-scale technological system dimension of critical infrastructures, their wicked nature, and crucially, their organizational attributes and dynamics is vital to identifying both the structural and policy issues that can lead to better, if not definitive, solutions. Critical infrastructure protection needs to be understood not only as deploying a tougher "exoskeleton" of infrastructure hardening and counter-terrorist anticipation, but also organizational "antibodies" of reliability that enable society to be more resilient and robust in the face of new, dynamic, and uncertain threats and contingencies.

ACKNOWLEDGMENT

This research was supported by a grant from the Critical Infrastructure Protection Project, George Mason School of Law.

NOTES

1. For a discussion of large technical systems, see, e.g., Mayntz et al. 1988.
2. Perrow 1984 (2nd edition 1999).
3. Zuboff 1988.
4. Michel-Kerjan 2003.
5. See Tucker 1999; Tucker and Sands 1999.
6. See National Center for Infectious Diseases 1999.
7. Turner 1976. Turner expanded on this in a book-length study. See Turner 1976, 1978.
8. On organizations not learning from their environments, see also Crozier 1964.
9. For example, traditional telephone systems provide their own electric power to run the public telephone network and have back-up batteries capable of keeping the systems functioning for about six hours. Electric power system operators have their own telecommunications networks to coordinate geographically dispersed operations, and the reliability operatives in the system have their *own* telecommunications system because they are concerned that the regular corporate network is not adequately managed for their needs.
10. For a discussion of the challenge of transformer replacement, see Chapter 13 of this volume.
11. Roe et al. 2002; U.S.–Canada Power System Outage Task Force 2004.

12. For a discussion of these characteristics within the case study of the 2001 anthrax attacks, see Chapter 25 of this volume.
13. Ritte and Webber 1973; Roberts 2001.
14. The first reference to private sector ownership of 85 percent of infrastructure appears to be in remarks by Sen. Robert F. Bennett on September 25, 2001, following his introduction of S. 1456, *Critical Infrastructure Information Security Act of 2001,* introduced in the U.S. Senate on September 24, 2001. See Bennett's remarks at http://bennett.senate.gov/press/record.cfm?id=226479, accessed October 7, 2005. See also President's Council of Advisors on Science and Technology 2002; Office of Homeland Security in the Office of the President 2002.
15. Wildavsky 1988.
16. Wildavsky 1988, 79–80.
17. Wildavsky 1988, 80.
18. The "high reliability organization" literature is identified mainly with researchers at the University of California at Berkeley and Mills College in Oakland, California. For other perspectives on the composition of high reliability organizations, see Chapters 8 and 9 in this volume. See also Rochlin et al. 1987; La Porte and Consolini 1991; Roberts 1990a; Schulman 1993a; Schulman 1993b; Rochlin 1996; La Porte 1996. For "mindful organization" literature, see Weick and Sutcliffe 2001.
19. Rochlin et al. 1987.
20. See La Porte, Todd R., 1996, for more detailed discussion of these points.
21. Rochlin 1993b.
22. The personal dynamics of trying to maintain the ability to "have the bubble" are well illustrated in the film, *Pushing Tin,* 1999, directed by Mike Newell, based on Frey 1996.
23. See Chapter 9 of this volume and Schulman et al. 2004; Schulman and Roe 2004.
24. Schulman 1993b.
25. Roe et al. 2002; U.S.–Canada Power System Outage Task Force 2004.
26. Grabowski and Roberts 1997.
27. Grabowski and Roberts 1997.
28. Little 2002; Heller 2001.
29. The literature on network modeling and simulation is growing rapidly. For examples, see Gorman 2004; National Infrastructure Simulation and Analysis Center 2003.
30. Fairley 2004.
31. Pressman and Wildavsky 1984.
32. Peters 1998.
33. Kettl 2004.
34. Kettl 2004, pp. 97–117.
35. Peters 1998.
36. Kauffman 1993.
37. Comfort 2002a. See also Comfort 2002b.
38. Rittel and Webber 1973, p. 162.