Critical Thinking:
Moving from Infrastructure Protection to Infrastructure Resilience

CIP Program
Discussion Paper Series

February 2007

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

The Critical Infrastructure Protection Program

The CIP Program leverages the considerable resources of academia to enhance the preparedness, protection, and resilience of the nation's critical infrastructure and key resources by leading scholarly discussion, promoting industry awareness, and providing support for public and private sector efforts. Under the leadership of John A. McCarthy, Director and Principal Investigator, the CIP Program has become a nationally and internationally recognized program through support from National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Department of Energy (DOE), and the National Capital Region. Mr. McCarthy has distinguished George Mason University as a center for excellence in critical infrastructure, recognized by over nine countries, the Department of Defense, DHS, DOE, and the private sector.

Current initiatives include:

- Supporting the national infrastructure agenda, the Commonwealth of Virginia, and regional and local communities.
- Leading scholarly discussion, promoting industry awareness, and providing support for public and private sector efforts.
- Creating forums to define the strategic legal and economic issues that impact critical infrastructure and homeland security.
- Conducting basic and applied research to further the national research agenda, specifically in cyber security, physical security, and information sharing between public and private sectors and regional, state and local entities.
- Applying research to develop solution sets needed to inform policy and decision makers on all levels.

Series Outline

The goal of this working paper series is to point out trajectories of the concept of critical infrastructure resilience in theory, policy, and implementation. On the one hand, “resilience” may just be another policy buzzword; but on the other hand, it might indicate a shift in perception and priority of threats, vulnerabilities, and consequences. Indeed, the Critical Infrastructure Task Force (CITF) has recently recommended to the Homeland Security Advisory Committee (HSAC) to “Promulgate Critical Infrastructure Resilience (CIR) as the top-level strategic objective - the desired outcome - to drive national policy and planning.”

Defined broadly as the ability of a system to withstand to and recover from adversity, resilience is increasingly applied to larger social and technical systems. Stress and adversity are experienced not only by individuals and groups, but also by organizations and institutions. In the context of increasing natural and man-made threats and vulnerabilities of modern societies, the concept seems particularly useful to inform policies that mitigate the consequences of such adverse and potentially catastrophic events.

Acknowledgment

This research was supported by the Critical Infrastructure Protection Program (CIPP) at George Mason University School of Law, which is funded through grant #60NANB2D0108 from the National Institutes of Standards and Technology (NIST). Any opinions, findings, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NIST or CIPP.

Table of Contents

Introduction

From Protection to Resilience: Injecting “Moxie” into the Infrastructure Security Continuum.

John A. McCarthy

Director and Principal Investigator
Critical Infrastructure Protection Program
Research Professor
George Mason University School of Law
Arlington, VA

A role of academe is to help define, clarify, and set boundaries for intellectual discourse. Academic partners can help impose needed rigor and discipline into the discussion of complex issues for decision-makers, helping to guide the public-private dialogue resulting from a post-9/11 homeland security environment. In this dynamic environment, objective forces can promote common understanding and are needed to enhance the preparedness, protection, and resilience of the Nation’s critical infrastructure and key resources (CI/KR). It is in this spirit the following papers are offered.

While sports analogies are often overworked and underserved, in this case, I believe that a sports analogy is appropriate for considering the elements necessary to advance CI/KR resilience.[1] After a boyhood of listening closely to my father’s analysis of various professional boxers and learning the sport’s terminology, I see the critical role that resilience plays in securing a boxer’s long-term success. I submit that resilience has a similar function in assuring the security of our Nation’s 17 CI/KR sectors.

Protective measures – a boxer’s glove work, footwork, tucking, and ducking – and robustness – his endurance, reach, and stamina or ability to “go the distance” – account for much of his skill sets, but resilience is an equally crucial element. Here, the idea of resilience is two-fold: 1) recovering from an immediate punch and continue the fight in the short-term, and 2) losing a fight, but having the ability to recover and continue fighting in the long-term. My father often summed up this critical aspect of a boxer’s makeup as “moxie”. As brutal as the sport might be, it offers a good metaphor for thinking about infrastructure security; without resilience, moxie, a boxer's long-term effectiveness is in question – his technical skills and stamina *will* fail him at some point – only moxie will assure the boxer will fight again. Similarly, without resilience, the infrastructure security continuum is incomplete.

The goal of this discussion paper series, **Critical Thinking: Moving From Infrastructure Protection to Infrastructure Resilience**, is to outline the concept of critical infrastructure resilience (CIR) in theory, policy, and implementation. Considerations of infrastructure security are evolving to include both critical infrastructure protection (CIP) and CIR. As this evolving process plays out, shifts in policy making, risk management, and approaches to threat, vulnerability, and consequence are also occurring. As government approaches infrastructure security with a greater focus on all-hazards, meaning both natural and man-made disasters and terrorism, the importance of CIR as well as critical infrastructure assurance[2] should receive greater attention and consideration.

While the topic of infrastructure security, and particularly critical infrastructure protection, has increased in visibility in recent years, the focus on CIP does not address all aspects of securing our Nation's critical infrastructure. Specifically among infrastructure owners and operators and our citizenry, CIP does not fully instill confidence in the security of our systems, networks, and assets. In order to infuse this critical confidence throughout our Nation and to achieve our overarching goal of building critical infrastructure assurance, we need to further pursue critical infrastructure resilience.

Resilience: The Present Landscape

Currently used as a buzzword and as homeland security "comfort food," resilience has not yet been fully recognized as a distinct concept within the infrastructure security continuum. Resilience is commonly embedded in processes, rather than individual physical assets (the main focus of protective measures and robustness) explicitly addressed in homeland security strategic plans, infrastructure protection programs, and the like. As an important long-term concept for homeland security, resilience should not be blurred to such a degree that its development becomes subverted and its importance as a construct becomes diluted. Rather, in an effort to reach the larger objective of building full confidence in the security of infrastructure, resilience needs to be studied further as a stand alone concept.

Yet, unlike protection,[3] resilience is not a specific, easily definable term across all infrastructures, nor is it easily measurable. Commonly defined as the ability of a system to recover from adversity, either back to its original state or an adjusted state based on new requirements,[4] building resilience requires a long-term effort involving reengineering fundamental processes, both technical and social.

While it may take time, improving the resilience of certain critical infrastructure is of increasing importance. Strengthening our resilience is vital to maintaining the essential services we rely on daily. However, we must be clear about what we are doing. At a recent conference on resilience, I heard a senior state official argue that his state's decision to bury power cables in an area prone to hurricanes is a significant step towards realizing "regional resiliency". Was it? Or, was it a sound protective measure? Computer scientists speak of improved firewalls and anti-virus measures as enhanced protection. Many of them argue that enhanced resilience in information systems, for instance, will require a significant research and development (R&D) investment in such concepts as automatic and self-healing networks. Regardless of various arguments on *how* to enhance resilience, it is evident that resilience must be taken into strong consideration when performing risk analyses, allocating resources and assets, and engaging in R&D initiatives.

Risk and Resilience

There are gradations of resilience within the risk chain, and thus, the manipulation of any portion of the risk chain, whether threat, vulnerability, or consequence, will cause the resilience of a system, network, or asset to change. Ultimately, a more resilient infrastructure proves better able to recover from natural and man-made disasters, less susceptible to disruption, and thus, less attractive to terrorist attack. Proactively addressing the elements of the risk chain can positively impact resilience. For example, enhancing resilience through an increase in redundancy, whether by installing additional fiber optic lines for telecommunications or utilizing additional facilities for energy production, can reduce threat and minimize certain consequences to operations or services. Thus, implementing redundancy will enhance resilience and serve to better sustain critical assets and systems.

For particular critical infrastructure sectors, understanding resilience can also inform decision-making about the best type of risk assessment methodology to use and where to invest scarce resources to ensure the greatest risk reduction. For instance, some assessment tools may be appropriate for those CI/KR sectors where protective measures may be easily identified and implemented, such as in the Transportation Sector. The performance of the Transportation Sector's highway infrastructure is influenced, e.g., by the number of people using it at a given time as well as by any motor vehicle accidents disrupting normal traffic patterns. Focusing protective measures on this kind of infrastructure can help prevent considerable disruption of services. However, "millisecond" sectors, such as Banking and Finance, Information Technology, and Telecommunications, require significant attention to resilience. Operating at the speed of light, these information-based sectors, given their self-healing systems and networks, require an emphasis on resilience, diversity, and redundancy rather than a greater focus on protection. Thus, acknowledging the role of resilience could drastically improve the security landscape for many critical infrastructure owners and operators.

Resources for Resilience Efforts

The innumerable interdependencies among infrastructures and linkages between elements of the risk chain require that consideration be given to resilience when both allocating resources to better protect non-resilient or less resilient infrastructures and prioritizing those assets that are most important to protect.

Funds allocated through the Fiscal Year 2006 U.S. Department of Homeland Security Infrastructure Protection Program, which includes various security grants, will enable select critical infrastructure systems or assets to enhance their security posture. As these grants are not specifically focused on resilience, and the fact that private sector owns or operates approximately 85% of the Nation's infrastructure, individual owners and operators are left to gauge infrastructures' resilience and implement appropriate measures to help build that resilience. As owners and operators seek to enhance infrastructures' security posture, ensuring the development of a robust planning and resource allocation framework for infrastructure security – that includes distinct recognition of resilience – will further add confidence in the security of the broader critical infrastructure spectrum.

Research & Development for Resilience Initiatives

Shifting focus to infrastructure resilience will also require an infusion of R&D efforts. Such efforts should examine the entire security spectrum, from physical protective measures to the sharing of information regarding threats and suspicious activities, common vulnerabilities, and best practices to examining long-term consequences of disruption to businesses and communities.

Many critical infrastructure stakeholders in the public-private partnership arena are actively addressing resilience R&D through joint working groups. In the United States, Government Coordinating Councils and Sector Coordinating Councils, as well as the Partnership for Critical

Infrastructure Security (the private sector cross-sector council), are reviewing existing research and identifying gaps that must be filled to adequately meet the growing needs of those charged with securing critical infrastructure. These groups are turning to previous research and case studies, as well as proposals, for valuable input and points of consideration for future projects that may be tailored to particular sectors or responsible sector-specific agency use. Notably, resilience also continues to be studied in-depth outside the U.S.; the United Kingdom and other nations have included this concept in their national security goals for a number of years.[5] In order to address the infrastructure security needs of the next decade, we must clearly assess past and present R&D efforts to promote effective and meaningful endeavors for the future.

Moving Forward: From Infrastructure Protection to Infrastructure Resilience

The following authors focus on resilience as a long-term concept. Their approaches lend valuable insight to the discussion surrounding the larger security of the Nation's infrastructure.

In *Resilience in Organizations and Systems: Background and Trajectories of an Emerging Paradigm,* Dr. Christine Pommerening, Senior Research Associate at the Critical Infrastructure Protection Program located in the George Mason University School of Law, describes various theoretical approaches to resilience and its application to technical and social systems. Pommerening notes that increased coordination between the public and private sectors and the development of an all-inclusive framework for preparedness, response, and recovery will assist in building CIR. The intellectual history of resilience is illustrated through its usage in theories on organizations and large technical systems. Based on this history, the paper compares the emerging resilience paradigm to the existing protection paradigm for infrastructure systems.

Dr. Lewis Perelman, Senior Fellow at the Homeland Security Policy Institute, depicts resilience as a developing concept for those leading the debate on homeland security and critical infrastructure and asserts the need for greater understanding of the social construct as it relates to securing our infrastructure in his paper, *Shifting Security Paradigms: Towards Resilience*. Perelman presents an initial conception of an alternative, soft security path in the framework of national and homeland security policy, aiming toward "social resiliency" and addressing themes such as flexible response via self-organizing systems, as well as non-hierarchical models of internal and external risk communication.

Advocating resilience as a comprehensive preparedness approach to critical infrastructure involving elements of protection, response, recovery, and other components of homeland security, Dr. Paula Scalingi, President of The Scalingi Group LLC, outlines key examples of resilience initiatives, lending credit to the utilization of this approach at all levels of government and among members of public-private partnerships in her paper, *Moving Beyond Critical Infrastructure Protection to Disaster Resilience*, Scalingi argues that critical infrastructure resilience requires a different way of thinking about preparing for and managing disasters that results in a comprehensive, all-hazards, cross-sector, grassroots-to-national integrated approach, and describes the development of a resilience-oriented regional partnership program.

In *Measuring Resilience in Network-Based Infrastructures*, Mr. David Garbin, Senior Fellow at the Center for Information Technology and Telecommunications of Mitretek Systems, and Dr. John Shortle, Associate Professor of Systems and Engineering and Operations Research at George Mason University, move the resilience discussion toward specific types of infrastructures by examining resilience in terms of network-based infrastructures. Garbin and Shortle describe interdependencies and critical nodes to demonstrate the cascading effects of systems degradation and the importance of network resilience and tailored risk assessments, and they outline an approach for quantitatively measuring a network through a resilience index. The authors identify research areas related to such measurements, and the need to gather data on a national scale on critical network elements such as utility rights-of-way. Garbin and Shortle further argue that a resilience index is crucial in establishing the business case for specific network improvements.

Mr. David Arsenault and Dr. Arun Sood, both of George Mason University's Department of Computer Science, elaborate on the need for tailored approaches to infrastructure security, as well as solid understanding of interdependencies, through their discussion of information systems and related networks in *Resilience: A Systems Design Imperative*. This paper introduces resilience as the primary characteristic of a holistic, "system of systems" architecture approach. The authors posit that modern networked systems in general, and information systems in particular, exhibit brittleness on a large scale due to the risks and challenges posed by three convergent forces—connectivity, complexity, and interdependence. A functionality-performance tradeoff curve is used to describe the behavior of a resilient system over a range of operating conditions.

Mr. Darryl Moody, President and Chief Operating Officer of Resilient Corporation, argues in *The Need for Resiliency at the Corporate Level* that resilience must be maximized, especially within the private sector, to better protect and secure our Nation's infrastructure. His paper describes how the concept of resilience can be integrated into the performance measurement and regulatory compliance process of companies. Moody acknowledges the impact of Federal government activities on private sector advances in resilience, also noting that there exists a clear business value for resilience. In this business-level perspective, resilience is both means and end, and thus, Moody argues, provides the building block for increasing overall societal resilience.

It is my hope that this work adds to current discussions on resilience and I look forward to any feedback. Please direct feedback to Dr. Christine Pommerening, Critical Infrastructure Protection Program, at 703-993-3132 or cpommere@gmu.edu.

For information on CIP and other topics of interest, please visit the website of the Critical Infrastructure Protection Program at http://cipp.gmu.edu/

Notes

[1] The terms "resilience" and "resiliency" are often used interchangeably, although they have the same definition in this discussion.

[2] Critical infrastructure assurance is a concept similar to that of critical infrastructure protection and critical infrastructure resilience. Critical infrastructure assurance implies full confidence in the security and continuity of CI/KR operations. This concept was explored in great depth by the U.S. Critical Infrastructure Assurance Office (CIAO), created following the issuance of Presidential Decision Directive-63 and later incorporated into the U.S. Department of Homeland Security.

[3] "Protection" includes "protective measures", which refer to actions, procedures, or physical impediments used to mitigate vulnerabilities, minimize consequence, and reduce risk. Simply put, protective measures are implemented to defend against harm to property, personnel, or mission execution. Examples of protective measures include, but are certainly not limited to, the following: surveillance cameras, security patrols and response capabilities, fencing, employee and visitor credentialing, and intrusion detection systems.

[4] The exact definition of resilience may vary in different contexts. The papers in this series, primarily those by Pommerening, Perelman, and Moody, provide additional background on this terminology.

[5] Homeland Security Advisory Council, "Summary of Meeting Held on June 23, 2005." (June 23, 2005). Available online at: http://www.dhs.gov/xlibrary/assets/HSAC_MtgMinutes_June23-05.pdf.

Resilience in Organizations and Systems. Background and Trajectories of an Emerging Paradigm.

Christine Pommerening

Senior Research Associate
Critical Infrastructure Protection Program
George Mason University School of Law
Arlington, VA

Introduction

In early 2006, the Critical Infrastructure Task Force (CITF), in a presentation to the Homeland Security Advisory Committee (HSAC), recommended to "Promulgate Critical Infrastructure Resilience (CIR) as the top-level strategic objective – the desired outcome – to drive national policy and planning."[1] This statement seems to indicate a new perception and prioritization regarding the threats, vulnerabilities, and consequences to critical infrastructures. If implemented, this would likely mean a major shift in deciding what constitutes the security of a system or a community, and, subsequently, what federal, state, and local as well as private measures would be supported.

On the one hand, "resilience" may just be another policy buzzword. Homeland security and critical infrastructure protection policy is a relatively new and constantly changing field. In part, this is due to relative newness of the notion that certain technological systems and economic sectors are at the same time vulnerable and vital for the security and safety of a society. In part, this is owed to the fact that every major event seems to challenge previously held ideas about how best to prevent, prepare, respond, and recover from natural or man-made disasters. In addition, the institutional framework is still evolving, too. All three branches of government are in the process of finding an appropriate legislative, jurisdictional, and administrative framework for homeland security.

At the same time, long-term perspectives and strategies need to be developed and justified. For that purpose, public policy relies on input from long-established academic disciplines such as organizational theory, political science, engineering, and law and economics. In fact, resilience is a well-researched concept that can be found in social psychology, organizational theory, and network science.

Defined broadly as the ability of a system to withstand to and recover from adversity, resilience is increasingly applied to larger social and technical systems.[2] Stress and adversity are experienced not only by individuals and groups, but also by organizations and institutions. In the context of increasing natural and man-made threats and vulnerabilities of modern societies, the concept seems particularly useful to inform policies that mitigate the consequences of such adverse and potentially catastrophic events.

The question is now how can these insights from various disciplines help in defining the concept of resilience for homeland security, and how does it relate to critical infrastructure protection in particular. In order to address these questions, this paper is divided into three parts. After this introduction, a literature review outlines the intellectual history of the concept through its usage in theories on organizations and large technical systems. Then, the emerging resilience paradigm will be compared to the existing protection paradigm for infrastructure systems. Lastly, an outlook section will look at the policy relevance of the conceptual insights.

Theoretical Approaches

The problem of effective coordination of disaster preparedness and response under conditions of uncertainty is similar to the problems addressed in organizational analyses of complex systems. In fact, many studies in this discipline use examples from public and private organizations that have to deal with natural or technological hazards, and use those case studies to explain factors influencing risk management and response capabilities. There is a large body of literature in the social sciences as well as operations research and engineering on various aspects of resilient systems. In this section, three examples will be discussed that are representative of prominent concepts in the social sciences: First, normal accidents theory, second, complex adaptive systems theory, and third, societal safety and risk perception.

Normal Accidents

Studies on the prevention of industrial accidents had traditionally been the domain of safety engineers. The dominant view was not that the engineered systems themselves could be inherently unsafe, but rather that shop floor conditions or operating errors lead to accidents, and that few if any negative externalities existed. Triggered by large-scale disruptions such as the accident at the nuclear power plant Three Mile Island in 1979, this view was challenged. In his 1984 book, Charles Perrow used insights from systems design, decision theory, and organizational theory to propose a theory on failure of systems and, more importantly for CIP purposes, recovery from failure (Perrow, 1984).

A system in this sense is an aggregation of components from units to parts to subsystems. Accordingly, "accidents" are also distinguished in ascending order from incidents to accidents to component failure accidents to system accidents. While the latter are by far the rarest events, with an empirical frequency of about 1% (based on his classification of Nuclear Regulatory Commission Licensee Event Reports), Perrow argues that these low probability/ high consequence events are the most instructive for understanding the multiple points of failure inherent in a system, as well as the equally manifold points of potential pre- or post-event intervention.[3]

Aside from the considerable influence that Perrow's work has had on disaster research and science and technology policy, his work is particularly instructive to the CIP community since he examines systems that are today considered part of a number of critical infrastructure sectors.

Perrow distinguishes systems in degrees of a) complexity and b) coupling, and failures caused by system properties rather than human errors in either design or operation. The eponymous normal accident theory (NAT) thus describes system accidents that "involve the unanticipated interaction of multiple failures (p.70)."[4]

Linear systems are characterized by spatial proximity, common-mode connections, interconnected subsystems, limited substitutions, feedback loops, multiple and overlapping controls, indirect information, and limited understanding. Examples include nuclear plants, as well as universities. Complex systems are characterized by spatial segregation, dedicated connections, segregated subsystems, easy substitutions, few feedback loops, single-purpose and segregated controls, direct information, and extensive understanding. Examples include dams, rail transportation, as well as the post office.

Tight coupling is associated with time-dependent and invariant processes with deliberate buffers and little, if any, slack; resources cannot be substituted easily or at all. Loose coupling means output delays are possible and the order of processing can be changed. In such systems, alternative methods and redundant resources are available, and fortuitous buffers and substitutions are possible.

A good example for most of these tendencies is different types of power plants. Nuclear plants are tightly coupled because the sequences are highly invariant, personnel need to be highly trained, and no substitute energy source can be utilized. In contrast, a coal-fired plant can operate with high or low stockpiles of coal, and it can even be switched to other fossil fuels entirely with relatively small adjustments.

The CIP relevance of the coupling concept is that it combines engineering logic with organizational theory in examining the responsiveness of systems to failures and shocks. Understanding a human or technical system's tendencies can help plan the response. There is no ex-ante better or worse type of system, however. While loosely coupled systems can incorporate shocks and pressures without destabilization because they are somewhat uncontrollable to begin with, tightly coupled systems will respond more quickly to change or disruption, but that response may very well turn out to be disastrous. As Perrow puts it "Both type of systems have their virtues and vices (p. 92)."

The important point is that since failures occur in both systems, the means to recovery are critical. Simply put, in tightly coupled systems, the buffers and redundancies and substitutions must exist already and be part of the design, while in loosely coupled systems there must be an ability to create solutions on the spot and exploit the system.[5]

Complex Adaptive Systems

Coordinating the response to a low-probability/high-consequence event that affects a complex system such as a critical infrastructure is not only a problem of private industry, but often affects public authorities as well. Nowhere was this more dramatically evident than during and after the events of September 11, 2001.[6] Public managers are confronted with increasing risk of potentially catastrophic disruptions in their jurisdiction, and need to strengthen the internal capacity of their organizations to prepare for and respond to disasters. In addition, they need to manage the interaction with private and nonprofit organizations to protect a community at risk from natural or technological disasters or terrorist attacks. While instruments such as the National Response Plan (NRP) and the National Infrastructure Protection Plan (NIPP) are supposed to enable this coordination, they clearly reflect the constraints on decision processes under uncertainty and illustrate the persistent difficulty in achieving coordination among multiple organizations with different responsibilities in different locations.[7]

This type of problem is discussed in complex adaptive system (CAS) theory. Essentially, it promotes a view of systems as being designed with an ability to adapt to change under conditions of uncertainty – in short, resilience.

In the field of public administration theory, Louise Comfort has examined several cases of disaster planning and recovery.[8] She argues that when public response organizations are under pressure, three elements characterize the types of adaptation to fast-changing conditions. Technical indicators (e.g. reliability), organizational indicators (e.g. communication and leadership styles), and cultural indicators (e.g. openness). They vary in degree from non-adaptive to emergent-adaptive to operative-adaptive, and, ideally, auto-adaptive systems. Achieving an auto-adaptive system would require public investment in an information infrastructure that can support the intense demand for communication, information search, exchange, and feedback.

For the management of critical infrastructure systems, the CAS view means that the complexity of public and private sector organizations and the uncertainty of risks (threats, vulnerabilities, and consequences) make a linear process of planning, preparedness, response, and recovery impossible. Instead, the best way to reduce risk would be focusing on the adaptability or resilience of response organizations.

However, Comfort also recognizes the tension between preparedness (or anticipation) on the one hand and resilience on the other as a means to reduce risk.[9] Depending on the information available before, during, and after an event, both the internal relationships in an organization and the external relationships between the system and its environment may change. Her case study of the inter-organizational disaster response system that evolved following the 1994 Northridge Earthquake showed that striking the balance between preparedness and resilience, order and chaos, is less a matter of an ex-ante planning document or policy decision that stresses the one over the other. Instead, she contends that structuring a process for continuous organizational learning is the primary requirement for maintaining creativity and adaptation when faced with catastrophic events.

Using the notion of complex adaptive systems and their inherent unpredictability, some authors have started to reexamine traditional risk management approaches. In a study on security, resilience, and communication in unpredictable environments, Longstaff addresses the underlying logic in various risk assessment, risk management, and risk communication concepts and strategies in the context of CAS (Longstaff, 2005). In addition to the common risk variables of threat, vulnerability and consequence or criticality, he examines the meaning of related but often underestimated phenomena. He contends that the rather clinical term “threat” disguises perceptions of danger, uncertainty, and surprise, while “vulnerability” hints at an inherent fragility that is impervious to engineering solutions such as redundancy. The author then identifies two main coping strategies for dealing with terrorism, natural disaster, and technology risks: resistance and resilience. Resistance aims at keeping everything safe, such as implied by 'fire-resistant' building materials, and is useful when dangers can be anticipated. Prevention then is “resistance that keeps bad things from happening.” Resilience is defined here as “an individual's, group's, or organization's ability to continue its existence, or to remain more or less stable, in the face of a surprise, either a deprivation of resources or a physical threat."[10]

Longstaff further distinguishes between engineering resilience as an effort to make a system return to a pre-designed state of function after a disturbance, and ecological resilience as a capacity to persist and adapt under new circumstances (what he calls flipping into new states).

Societal Safety and Risk Perception

If we assume increasing internal complexity of systems as well as increasing external risks to such systems, then factors such as uncertainty, cognitive limits, and unintended consequences are likely to have an effect beyond their role in a particular organization, technical system, or disaster. In fact, they become important parameters for designing safety and security-oriented public policies per se. This link has been recognized early on by Aron Wildavsky. He examines how societal approaches to dealing with risk are often ineffective and counterproductive (Wildavsky, 1988). Generally, he argues, people try to anticipate dangers and then prevent them from causing harm, instead of trying to increase resilience by enhancing the ability to respond to unexpected dangers[11]. He argues that the focus should be shifted from this “passive prevention of harm to a more active search for safety.”

He proposes creating a balance of anticipation and resilience as a strategy for reducing risk in uncertain conditions. Anticipation means a careful assessment of vulnerability with prudent action taken to limit obvious danger. This anticipation strategy remains vital to protect against risks whose potential for realization is substantial. Resilience means a flexible response to actual danger, demonstrating an ability to 'bounce back' after a damaging event. This resilience strategy is most appropriate for dealing with unexpected events.

A combination of systematic actions to reduce known risk and the capacity to act quickly when faced with unexpected dangers is the most successful resilience strategy. However, this places a considerable burden on decision makers in that it requires reliance on experience with little recourse to external support.[12] On a macro-level, adopting the resilience strategy over the anticipation strategy would increase resources, public knowledge of actual versus perceived risk, and societal coping mechanisms.

Resilience in Perspective

The previous part of this paper outlined trajectories of the resilience concept in organizational and institutional theory, and thus attempted to better ground the debate about a paradigm shift from protection of assets and structures to resilience of organizations and systems. The following part tries to determine the policy relevance of the resilience paradigm. In particular, the comparison matrix provides a framework for analyzing the appropriateness of either the protection or the resilience approach along a number of criteria relevant to critical infrastructure systems. The example of an existing resilience-based security approach provides a reality check as to how closely traditional preparedness and response institutions are tied to a resilient community.

Criteria for Distinguishing Protection and Resilience

The following table lists a number of criteria by which the appropriateness of protection measures versus resilience measures could be assessed. Just as a linear or a complex system is not better or worse but different, the corresponding measure is not better or worse, but appropriate or inappropriate. In other words, depending on the context, resilience is not necessarily the only option for infrastructure security. The key is recognizing how e.g. the nature of the system, the budget needs, or the subject in question, would point to a differentiated approach.

Table 1. Protection and Resilience

	Protection	**Resilience**
Activity planned	hardening structures	redesigning processes
Subject focus	asset-driven	services-driven
Desired metrics	absolute (0/1)	conditional (0-1)
Value proposition	cost-centered	benefit-centered
Security stance	reactive approach	proactive approach
Type of disturbance	(sudden) disruption	(graceful) degradation
Budget needs	short-term investments	long-term investments
Network character	insulated	interdependent
System interaction	linear	complex
System coupling	loose	tight

To illustrate how protection and resilience are no absolute categories, but depend on the type of system and problem at hand, power generation provides a good example. For example, if an electric power plant did not have a perimeter fence, the activity associated with that would be hardening the structure – a protection measure. The same company might identify the need to have a contingency staffing plan that assigns and trains substitutes for critical functions – a resilience measure. If it is a conventional plant, it is loosely coupled in terms of its energy supply, meaning it is possible to switch to another fuel if the primary source is disrupted (e.g. from oil to coal). Stockpiling such a reserve is thus a simple protective measure. However, if it were a nuclear plant, the tight coupling would require different measures to cope with disruption in its fuel source; a stockpile of coal would be useless. Moreover, because of the complexity of dealing with nuclear material, such a fuel source disruption would impact all other operations in the plant. Of course, technological systems are constantly evolving, meaning that an environment such as a conventional power plant in which protection measures used to be sufficient may have changed to the point that resilience measures have become necessary.

It can be argued that in the case of power plants, the extensive adoption of supervisory control and data acquisition (SCADA) technologies has resulted in turning loosely coupled systems into tightly coupled ones, making them less failure tolerant. Finally, if the power company in charge is a public utility, it may not have long-term security investment funds because of limitations in its particular rate structure. If that were the case, and only ad hoc upgrades can be financed, it needs to be understood that the result of the expenditures will be protective measures, not resilience measures, regardless of the kind of system or activity planned.

Organizing for Resilience

The first large-scale institutional reorganization under the banner of resilience has been undertaken by the City of London.[13]

“London Resilience” is a strategic partnership of key emergency preparedness and response organizations and bodies in the British capital in both the public and private sectors. Created in 2001 in the wake of the 9/11 attacks in the U.S., its task is to ensure the preparedness of the Greater London area for major incidents or disasters. There are two main components: The London Resilience Team as operative arm, and the London Regional Resilience Forum as strategic leadership arm.

The London Regional Resilience Forum oversees the work of all London Resilience actions. It is composed of senior officials representing the main emergency organizations and key sectors within the partnership. It is chaired by the cabinet-level Minister for London Resilience, with the Mayor of London as deputy chair. The Forum reports directly to the Prime Minister and has a number of sub-committees and working groups that concentrate on particular aspects of the city’s preparedness. These include:

- Blue Lights (dealing with matters related to the emergency services)
- Utilities (dealing with matters affecting key utilities such as water, gas and telecommunications, some of which are municipally owned)
- Business (representing the private business community)
- Health
- Transport
- Communications (meaning emergency notification and media information)
- Local Authorities
- Voluntary Sector

The London Resilience Team is chartered with supporting those sub-committees, and the members are equivalent to lead agencies that represent each function listed above. As the main operative arm, this team consists of civil servants and private sector organizations with quasi-public functions. The team is based within the Government Office for London, and includes:

- The Metropolitan Police Service, the City of London Police, and the British Transport Police
- The London Fire Brigade and the London Ambulance Service
- The National Health Service
- Transport for London, and the London Underground
- The Government Information and Communications Service
- British Telecom
- The Greater London Authority
- Corporation of the City of London, Emergency Planning Department
- London Fire & Emergency Planning Authority
- The Salvation Army

This strategic emergency preparedness and response regime embodied in the concept of London Resilience was put to the test during the July 2005 London underground rail and bus bombings. During those incidents (four on July 7 with 52 fatalities, and four additional attempts two weeks later) the Commissioner of the Metropolitan Police took charge of the so-called “Gold Coordinating Group”, which brought together the top management of the London health service, local councils, emergency services, utilities, transportation and port authorities.

A detailed review of the effectiveness of response and restoration efforts is still being conducted, and it is difficult to estimate actual losses and costs.[14] However, the fact that most buses and trains were running and the city was ‘open for business’ again the very next day appears to have proven the validity of the concept of an emergency response that is oriented towards managing not only the immediate event but also reconstituting the indirectly affected systems and the community at large.

Summary and Outlook

From a structural point of view, critical infrastructures can be described as consisting of physical assets and networked systems that are operated by public and private sector organizations. As such, they fall into the analytical category of large technical systems which have been examined in organizational theory and political economy for more than three decades. While there are different theories on their functioning as outlined above, there are some common insights on these systems: They are highly complex and characterized by networks of organizations instead of single or discrete organizations, they exhibit large scales and scopes, and failures are typically not confined to individuals but affect the entire system. The parameters of their function and failure are thus technical as well as organizational and societal in nature.[15]

The question is what these observations on the nature of complex technologies and complex organizations can contribute to creating more resilient infrastructure systems? It seems that the strength of these approaches are also their shortcomings in that the focus on system properties such as tight or loose coupling (Perrow), and brittleness or robustness (Longstaff) leaves out non-systemic risks. Those are important parameters, but it seems that the basic difference between resistance and resilience strategies is epistemological in nature: Resistance requires knowledge of the threat, while resilience requires knowledge of the consequence.

There is growing agreement that the first, knowledge of threats, is difficult to achieve, and even more difficult to implement in form of appropriate protection measures. However, there is a curious disconnect between recommending coping and adaptation strategies for new stages of stability, and the fact that we have just as little knowledge about how those stages will look as we reliable threat information. Beyond stating the need for feedback loop learning and investments in knowledge management, there is little appreciation yet that even the best metrics and measures do not provide a holistic view of such new environments.

Organizational theory and disaster research provides vital insights into the behavior and complexity of the systems we want to protect and the organizations that manage them. For resilience to become a viable security paradigm, this is necessary but not sufficient. The work ahead lies in defining the range of possibilities and then agreeing on the acceptable level of what a resilient company, industry, and community will look like. What services at what costs can be expected from an energy company that invests in a resilient electricity grid? How can a government agency that is turned into an auto-adaptive system be held to uniform accountability and performance standards? If there is no 100% protection for everyone and everything at all times, what are the acceptable levels of lives lost (or saved) and of assets destroyed or recovered?

While these questions are yet unanswered, the example of London indicates that the resilience concept has at least the potential to merge previously separate spheres of public and private sector disaster planning, emergency response, and infrastructure restoration into a comprehensive framework for assuring the functioning of both individual systems and the community at large.

Notes

[1] See (David, 2006)

[2] There are numerous definitions of the term “resilience” or “resiliency.” One of the earliest and most often quoted suggestions is by Holling, who proposed that resilience is the capacity of a system to absorb stress or shock and return to a stable state (Holling, 1973). Wildavsky uses a very similar terminology, seeing resilience as the capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back (Wildavsky, 1988). Gunderson et al. have recently distinguished engineering resilience and ecological resilience (Gunderson, Holling, Pritchard, & Peterson, 2002); with engineering resilience as the speed of return to a steady state following a perturbation, and ecological resilience as the magnitude of disturbance that can be absorbed before the system restructures. Finally, the National Infrastructure Protection Plan defines resiliency as the capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack or other incident (U.S. Department of Homeland Security, 2006a).

[3] “Normal” accident is thus a bit misleading; it does not refer to the frequency of failures and is different from everyday or routine accidents.

[4] Clearly, this eliminates a large number of causes for system failures, and does not even mention intentional sabotage or attacks. He also explicitly excludes so-called “final accidents” that completely destroy a system, for example a dam hit by an earthquake.

[5] In what could be called the “glass half full” version of Perrow’s “glass half empty” view of system failure, there is a body of work that asserts that certain organizational structures can contribute significantly to the prevention of disasters. Interestingly, these so-called high-reliability organizations (HRO) often coincide with high-risk environments such as nuclear power plants and ships They are characterized by high levels of technical competence and sustained performance, rewards for error discovery and correction, decentralized authority patterns, structural redundancy, and adequate and reliable funding. For further reading, see e.g. (La Porte & Thomas, 1994), (Frederickson & La Porte, 2002), and (Schulman, Roe, van Eeten, & de Bruijne, 2004).

[6] But even before that, numerous studies have examined the role and performance of government agencies in disaster preparedness and response; see e.g. (Comfort, 1994; Waugh Jr, 1994; Weick, 1993)

[7] Those planning documents contain a mix of best practices, anecdotal examples, organizational directives, and incident management system outlines for coordinating federal, state, and local authorities, and private sector entities to plan, prevent, respond, and recover in the case of incidents of national significance (U.S. Department of Homeland Security, 2006a, 2006b).

[8] See (Comfort, 1994, 2002; Comfort, Sungu, Johnson, & Dunn, 2001)

[9] Comfort uses the terminology introduced by Wildavsky; see discussion below.

[10] Longstaff, 2005; p.25-27

[11] Wildavsky uses the terms danger and damage instead of threat and consequence when analyzing risk. “Anticipation is a mode of control by a central mind; efforts are made to predict and prevent potential dangers before damage is done… Resilience is the capacity to cope with unanticipated dangers after they

have become manifest, learning to bounce back… Anticipation seeks to preserve stability: the less fluctuation, the better. Resilience accommodates variability; one may not do so well in good times but learn to persist in the bad."

[12] (Comfort et al., 2001)

[13] London Resilience became the basis for the Civil Contingencies Act of 2004, which places a legal obligation upon emergency services and local authorities to assess the risk of, plan for continuity in case of, and exercise preparing for emergencies, as well as undertake contingency planning (see Office of Civil Sector Information. (2006). *Civil Contingencies Act 2004*. Available at http://www.opsi.gov.uk/acts/acts2004/40036--b.htm#1)

[14] The general consensus is that the economic impact for London, the UK, and worldwide financial markets is minor. Forecasts for the British tourism industry for example were corrected downwards by less than 2% overall (see World Travel and Tourism Council. (2006). *World Travel & Tourism Council Crisis Committee Issues Estimate of London Bombing Impact.* Available at http://www.hotel-online.com/News/PR2005_3rd/July05_LondonImpact.html). In addition, many estimates assume that production or consumption is completely lost, while in reality it is often only deferred in terms of time or location.

[15] Shrivastava et al have coined the acronym HOT resilience, meaning the resilience of a system is defined across its human, organizational and technological (HOT) components (Shrivastava, Mitroff, Miller, & Miglani, 1988).

References

Comfort, L. K. (1994). Risk and Resilience: Inter-Organizational Learning Following the Northridge Earthquake of 17 January 1994. *Journal of Contingencies and Crisis Management, 2*(3), 157-170.

Comfort, L. K. (2002). Managing intergovernmental responses to terrorism and other extreme events. *Publius, 32*(4), 29-40.

Comfort, L. K., Sungu, Y., Johnson, D., & Dunn, M. (2001). Complex Systems in Crisis: Anticipation and Resilience in Dynamic Environments. *Journal of Contingencies and Crisis Management, 9*(3), 144.

David, R. (2006). *Critical Infrastructure Task Force Presentation to Homeland Security Advisory Council.* Retrieved February 15, 2006, from www.dhs.gov/dhspublic/interweb/assetlibrary/CITF_Report_HSAC_Bl.pdf

Frederickson, H. G., & La Porte, T. R. (2002). Airport security, high reliability, and the problem of rationality. *Public Administration Review*, 33-43.

Gunderson, L. H., Holling, C. S., Pritchard, L., & Peterson, G. D. (2002). Resilience of Large-Scale Resource Systems. In L. H. Gunderson & L. Pritchard (Eds.), *Resilience and the Behavior of Large-Scale Systems.* (Vol. SCOPE Series Volume 60.). Washington, DC: Island Press.

Holling, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*(4), 1-23.

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

Longstaff, P. H. (2005). *Security, Resilience, and Communication in Unpredictable Environments such as Terrorism, Natural Disasters, and Complex Technology*. Cambridge, MA: Harvard University.

Perrow, C. (1984). *Normal Accidents: living with high-risk technologies*. New York: Basic Books.

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

Shrivastava, P., Mitroff, I., Miller, D., & Miglani, M. (1988). Understanding industrial crises. *Journal of Management Studies, 25*(2), 283-303.

U.S. Department of Homeland Security. (2006a). *National Infrastructure Protection Plan (NIPP).* Washington, DC: U.S. Department of Homeland Security.

U.S. Department of Homeland Security. (2006b). *National Response Plan (NRP).* Washington, DC: U.S. Department of Homeland Security.

Waugh Jr, W. L. (1994). Regionalizing emergency management: counties as state and local government. *Public Administration Review*, *54*(3), 253-258.

Weick, K. E. (1993). The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster. *Administrative Science Quarterly*.

Wildavsky, A. (1988). *Searching for Safety*. New Brunswick, NJ: Transaction Books.

Shifting Security Paradigms: Toward Resilience.

Lewis J. Perelman

Senior Fellow
Homeland Security Policy Institute
Washington, DC

Resilience has been a progressively crystallizing theme as the U.S. and other nations have grappled with the dilemmas of 'homeland security' in what often has been called the 'post-9/11 world.' What resilience (or resiliency) means in discussions of security strategy is variable and often cloudy. But the notion of resilience as an organizing doctrine continually appears as a counterpoint to the typical, reflexive actions of governments to defend their territory and people against catastrophic attacks, natural disasters, or industrial accidents.

The allure of resilience is stoked by the contradictions and thorny tradeoffs inherent in traditional concepts of 'national security' in an age of increasing social-technical complexity, transnational 'globalization,' and 'asymmetric' conflict. Certainly, 'homeland security' has realized, since 2001, both political impetus and bureaucratic mass. Nevertheless it has been fraught by a tumultuous and yet unresolved quest to reconcile legitimate but competing social objectives:

- Security against attacks vs. security against natural disasters, disease, accidents, etc.;
- Intelligence operations vs. privacy;
- War-fighting vs. human rights, civil liberties, the rule of law, etc.;
- Needs for secrecy vs. needs for information sharing;
- Federal responsibility vs. state/local/private authority;
- Centralized command and control vs. communal collaboration.

As the alignment of the above examples suggests, these and similar dichotomies are not self-contained but cluster within broad constellations that represent two common but fundamentally different human impulses about the problem of security.

In purest form, one seeks the *prevention* of harm, through the elimination of risk and uncertainty. The other, accepting the irreducibility of risk and uncertainty, seeks *adaptation* through flexibility and agility. The first aims for triumph; the second aims for endurance.

Within this social dialectic over security strategies, the snowballing interest in resilience should not be viewed merely as a rhetorical finesse of established practice, albeit that the words 'resilience' and 'adaptation' can be and have been used as just new labels on old wine. Rather, behind the rhetoric of 'resilience' and 'adaptation' is an insurgent, alternative vision contending for the leadership of social policy.

Two Paths

The reptilian brain of today's politics admits only two views of 'national security', either *for* or *against*. Yet in reality, beneath the blare of the main media's political chatter, two basic conceptions—'paradigms' if you will—of national security have been crystallizing:

- the *hard* paradigm or path of conventional, established security policies and practices associated with prevention and resistance, and
- the emerging *soft* paradigm or path, associated with adaptation and resilience.[1]

Moreover, the schism of these alternative concepts of both the meaning and means of security has been evolving not just in the much-vaunted 'post-9/11 world' but at least since the early 1970s.

In response to the pinch of energy costs as U.S. domestic oil production began to peak out in 1970, President Richard Nixon lifted oil import quotas and abandoned the direct convertibility of the dollar to gold. The subsequent devaluation of the U.S. dollar angered 'third world' countries whose real incomes were reduced for the commodities they exported, most notably petroleum producers.

That anger boiled over during the Arab-Israeli 'Yom Kippur' War in 1973 when the Organization of Arab Petroleum Exporting Countries cut production, raised the price of oil, and embargoed oil exports to the United States and other countries perceived as supporters of Israel. By 1974 the economies of the U.S. and the world as a whole were thrown into a miserable melange of soaring inflation and deep recession.

In the midst of the 1970s crisis, the beginnings of a paradigm shift in thinking about not only energy but national economic and strategic security was broached by Amory Lovins in a benchmark article in the October 1976 issue of *Foreign Affairs*, "Energy Strategy: The Path Not Taken?"[2]

The crux of the paradigm argument presented by Lovins, a physicist affiliated then with Friends of the Earth, was sedulously but not completely technical. Lovins observed that, as represented by the Nixon and Ford administrations' Project Independence, the hard path aimed to feed growing energy demands while reducing dependence on foreign oil supplies through an aggressive, capital-intensive expansion of domestic energy supplies. Those goals were to be achieved chiefly by building more nuclear power plants, extending domestic oil production to previously undeveloped offshore and Arctic areas, and increased use of coal to generate electricity and to be converted to liquid and gaseous fuels.

As a security strategy, Lovins characterized the thrust of the hard path as a policy of "Strength Through Exhaustion."[3]

The soft path alternative proposed by Lovins rested on a few key premises. First, so much energy was being wasted in production, transmission, and conversion of energy resources that improved technical efficiencies in these processes could provide far more economic value with no more or even less gross energy consumption. Moreover, 'hard' technical systems were so capital-intensive, environmentally hazardous, and vulnerable to disastrous breakdowns that they threatened to subtract more from the economy than they added. But alternative 'soft' technical systems were readily available that cost less and could be implemented more swiftly and safely. Last but not least, the hard path's plan for expanded nuclear power would reduce overall national security by increasing the threat of nuclear weapons proliferation.

Fast forwarding to present-day concerns about national/homeland security, critical infrastructure, and, yet again, 'energy independence' and proliferation of nuclear/other 'weapons of mass destruction,' the conclusion of Lovins' case for a soft paradigm is instructive:

> …[T]he soft path appears generally more flexible—and thus robust. Its technical diversity, adaptability, and geographic dispersion make it **resilient** and offer a good prospect of stability under a wide range of conditions, foreseen or not. The hard path, however is **brittle**; it must fail, with widespread and serious disruption, if any of its exacting technical and social conditions is not satisfied continuously and indefinitely.[4]

Lovins was neither the first, last, nor only proponent of a 'soft' alternative to the dominant 'hard' paradigm of national security.[5] However, his 1976 essay contained the essential themes of a policy dialectic that has fermented and evolved through subsequent decades to our present struggle to find an effective balance between prevention and adaptation, between wars of force and wars of ideas, and between resistance and resilience.

Paradigm Contest: What it isn't

Before proceeding to an anatomy of the paradigm rift in today's national security policy debates, we should understand what the contest between the hard and soft paradigms is not.

It is not a competition between such conventional political stereotypes as conservative and liberal, right and left, Republican and Democrat. To follow the hard path or the soft path is not a choice between pro-military and anti-military or even necessarily pro-war and anti-war. Nor should the split between the hard and soft paradigms be equated with simplistic, cliched distinctions such as Industry vs. Environment or Technology vs. Human.

Rather, the hard paradigm may well reflect the inertial residue of the culture, economy, and reductionist logic of the bygone industrial age. And the soft paradigm, in contrast, seems to be more in tune with the postindustrial society that finally arrived with the new millennium. Where the hard paradigm at heart holds an intensely mechanical view of the world, the soft paradigm builds on a more nuanced understanding of sociotechnical ecology, informed by recent advances in chaos, complexity, and information theories.

The Difference: Hard vs. Soft

Since the end of the Cold War, and particularly since 9/11**,** national security affairs have so far lacked a coherent, organizing doctrine comparable to the Kennan theory of "containment" that framed Western strategic thought and action for over four decades.[6] The gap in coherent grand strategy has been filled to some extent by the inertial continuation of Cold War ideas and practices—even when rhetoric admits the limitations or obsolescence of those concepts—and ad hoc reactions to the latest threat or crisis. Nor do the US and its allies share a common strategic view.

Even if it may be more a 'bunch' than a 'system,' America's resulting hard security path—pursuing a kind of *social fortification*—has demonstrated some common themes. Aligned under the same set of key security issues, the soft security path—aiming toward *social resilience*—offers a tangibly different vision of reality and strategy.

Priority

Since the watershed event of 9/11, the hard security path followed by the U.S. government has given substantially higher priority to terrorist threats than to other kinds of threats or risks. This was despite the fact that the legislation creating the Department of Homeland Security and two official presidential directives explicitly called for an "all hazards" strategy. As the office of the department's inspector general noted in its review of the response to Hurricane Katrina in 2005, "After the terrorist attacks of September 11, 2001, DHS' prevention and preparedness for terrorism have overshadowed that for natural hazards, both in perception and in application."[7]

The soft path alternative to the superordinate priority given to terror threats is represented by calls for a balanced, "all-hazards" strategy of preparedness. Those calls were energized by the catastrophic consequences of the compound assaults on the U.S. Gulf Coast by hurricanes Katrina and Rita in 2005. The inadequacies of planning and response to that catastrophe evidently vindicated the warnings of critics who had opposed the legislation that subsumed the Federal Emergency Management Agency into the proposed DHS in 2002 on the grounds that "all-hazards" capability would lose out to the acute focus on terrorism.[8]

The Katrina-Rita disaster stimulated government efforts to redress the imbalance of narrow-focus programs in the direction of an all-hazards doctrine. For example, the National Earthquake Hazard Reduction Program lately has been revising its five-year strategic plan to broaden its single-purpose mission to embrace "multiple hazard" mitigation designs and measures.[9]

But from the soft-path perspective, this progressive adaptation of program plans demands a caveat: A "multiple hazards" strategy is not a reliable or adequate substitute for a true "all hazards" approach.

The process of selecting the multiple hazards for official attention necessarily implies excluding other hazards that will thus be ignored—creating blind spots and potential new vulnerabilities. The multiple-hazards approach therefore does not alleviate the 9/11 Commission's key complaints about the government's "failure of imagination" and inability to "connect the dots" in assessing and managing risks to public safety.[10]

Metaphorically, invulnerability to "all hazards" was Achilles' pride; invulnerability to "multiple hazards" was Achilles' heel.

Precisely because the soft path realizes that it cannot anticipate all possible hazards, it plans on the basis not just of what is known but on the expectation of surprises—'Black Swans' (highly improbable events) and UnkUnks (unknown unknowns).[11]

Protection

Within the established hard paradigm, particularly within the homeland security domain of 'critical infrastructure protection,' the operational concept of *protection* has emphasized (1) a focus on singular, concrete assets and (2) 'hardening' whatever is construed as 'critical' assets against a range of imaginable attacks or threats. There may be no other branch of the tree of national security missions that is more palpably 'hard' in its conventional conception. Granted that, it is misleading if not an error to view 'resilience' as an alternative to 'protection,' as has been done in some recent policy discussions.[12]

The soft paradigm, emphasizing adaptation and resilience, is not less interested in protection but rather addresses the mission with a different vision and philosophy. The relationship is somewhat analogous to the differences between the traditional dogma[13] of standard, Western allopathic medicine—which attacked discrete diseases with expertise specialized through particular organ, subsystem, or technical 'stovepipes'—and various 'alternative medicine' disciplines that take a more 'holistic' view of complex, living systems and focus more on health than the absence of disease. Both pursue the same human goal, but along distinctly different paths.

Within the security sphere, the emerging soft paradigm seeks protection along a path that is almost opposite to that of the hard (and hardening) path. First, it takes a holistic view of 'infrastructure' as complex, dynamic, adaptive, even living *systems*, rather than discrete, concrete, fixed *assets*.[14] And second, it aims at *softening* the brittleness of systems by reducing their vulnerability profile through redundancy, lower cost, dispersal, reduced scale, self-healing capability, accelerated repair/recovery, more 'graceful' failure modes, and so forth.[15]

Ultimately, it is the paradox of brittleness that dooms the doctrine of hardening, whether through prevention or protection, to self-defeat. As Patricia Longstaff of Syracuse University explains, both accumulated experience and advanced systems analysis reveal that the more "tightly coupled" complex systems are, the more brittle they become. [16]

The major power grid failure that struck the northeastern United States in the summer of 2003 is a relevant real-world example of the brittleness dilemma. An *IEEE Spectrum* report[17] found that while several university teams that analyzed the disaster disputed some technical issues, they all gravitated toward the same broad policy lessons: That the sheer scale and complexity of modern power grids makes periodic, disastrous failures inevitable. Moreover, the measures typically embraced by utility regulators and managers following a major blackout, to protect the system from a repeat of the disaster, actually tend to be ineffective or even to make future blackouts bigger and more likely.

The soft path's central lesson thus inverts a timeworn aphorism: *The harder they are, the bigger they fall.*

Concept of Risk

Risk is a key concept that substantially distinguishes the hard and soft security paradigms, especially in the homeland security domain. The hard paradigm uses a concept of risk that commonly is rooted in the 'hardest' disciplines of engineering, to the more or less complete exclusion of human factors—social, political, behavioral, psychological, and even some important economic factors.[18] The soft paradigm is far more attuned to these human factors, particularly in regard to social perceptions, communication, and public choice.

The key reality that the hard paradigm ignores—at considerable practical cost—is that "risk" in reality is a purely social construct. Common sense validates this: We do not invest any worrying in the "risk" of giant trees falling in the dark recesses of uninhabited rain forests or of avalanches roaring down the slopes of desolate mountains in central Antarctica. Where there is no effect on people, risk has no meaning.

Despite what common sense suggests, common practice within DHS and other homeland security bureaucracies has been to define "risk" by the following analytical equation:

Risk = **T**hreat x **V**ulnerability x **C**onsequences

But in social reality—the space where politicians, bureaucrats, investors, business executives, and other real people actually care about and seek to manage "risk"—this definition is incomplete, and thus false in a way that proves to be ironically 'risky' in practice. The right side of the above equation is a statistical compendium of what more accurately should be called "engineering failure," not "risk."

The soft path's more socially authentic, practical definition of "risk" would go something like this:

Risk = **HF**(**T**hreat x **V**ulnerability x **C**onsequences)

where **HF** is a function of the "soft" human factors that translate the "hard," physical parameters of engineering failure into human perceptions, emotions, and behavior.

Lester Lave of Carnegie-Mellon University is among the thought leaders who have urged public officials to adopt this more realistic understanding of risk, particularly in regard to counterterrorism:

> DHS needs to set priorities by the terror value of an attack, which is not the same as the amount of damage or number of people killed or injured.…[An] attack that kills people, even a large number of people, need not cause terror. At the same time an attack that killed no one could cause immense terror. Preventing an attack from causing terror requires recognizing that terror is an emotional, not a rational reaction and that people must be prepared for the attack.[19]

A crucial corollary to this social, realistic definition of "risk" is that human perceptions, emotions, and behavior vary among individuals, groups, and populations—and hence that "risk" is very much in the eyes (and hearts and minds as the saying goes) of the beholder. And that is not just a singular, generic, average beholder but a human ecosystem of diverse beholders, or "stakeholders" in the argot of policy wonks.

It follows that the problem of "risk management" is not one of managing physical assets or infrastructure but of managing human thoughts, feelings, and actions. That problem ranges from immensely complex to chaotic. But it is not impossible. It is, after all, what politicians, public officials, and private sector executives are required to do every day.

But it is just these human, social dimensions of the task to which the technocratic denizens of the hard security paradigm are commonly inattentive and often blind. The practical results of this social apathy have ranged from grave to farcical:

- Before Hurricane Katrina, official plans for emergency response and incident management focused on evacuating and rescuing people—to the exclusion of pets. Charged with the mission of saving human lives, tunnel-visioned planners perceived no rational reason to expend resources on rescuing animals. The result: "Thousands of survivors clung to their pets and refused orders from emergency workers to leave them behind. The holdouts included a number of older men and women living alone who elected to stay with their animals despite the harrowing conditions, a choice that cost some their lives."[20]
- A political firestorm erupted in February 2006 when news media reported that an arcane panel of federal technocrats, the Committee on Foreign Investment in the United States (CFIUS), had casually approved the purchase of six major American port facilities from their then-British owner by Dubai Ports World, a firm owned by the government of the Arab Emirate of Dubai. Public outcry led to congressional outrage that resulted in the transaction being stymied, and later revised to assure control of the six ports by a U.S. company. A number of analysts and government officials reasonably claimed that the backlash insulted a strong U.S. ally in the Arab world, seemed 'racist,' and undermined needed foreign investment.[21] However, they overlooked that the fiasco was generated by the government's own reliance on the mechanical concept of "risk management"—and its resulting egregious failure at effective "risk communication."
- In June 2006, a similar political backlash once again greeted the announcement by DHS that its latest round of anti-terrorism grants under the Urban Area Security Initiative (UASI) would cut funding to New York City and Washington, DC, by some 40 percent—colliding with the near-universal perception that New York and Washington continue to be the prime targets for pro-

spective terror attacks. Defending the decision—but without naming the members of the secret committee or the secret calculus from which it was derived—Secretary of Homeland Security Michael Chertoff boasted that the results demonstrated his department's commitment to rational risk management. "What we have to do," said Chertoff at a Brookings Institution symposium, "is manage the risk, and that means…evaluate consequence, vulnerability, and threat in order to determine what is the most cost-effective way of maximizing security."[22] I. Michael Greenberger, director of the Center for Health and Homeland Security at the University of Maryland, echoed a chorus of analysts, public officials, and congressional leaders when he told a reporter "the plan doesn't pass the common-sense test." [23] Indeed, it demonstrated yet again the counterproductive real-world impact of the reliance on utopian, technocratic concepts of risk, risk assessment, risk management, and risk communication.

While drifting, or perhaps hurtling, down the hard path, the United States has not—in the past five years at least and arguably since the seeming triumph of Operation Desert Storm in 1991—had a serious national conversation about what kind of 'security' Americans want, and at what price. The lack of a coherent rationale of the full spectrum of risks, costs, and benefits that affect the lives, welfare, and future aspirations of the American people has yielded a relationship between security and economy that is riddled with ironies…:

Some 90,000 people die every year in the United States from infections they acquire while being treated in a hospital for something else. Most of these deaths are preventable at the relatively small cost of getting hospital personnel to wash their hands. Yet the problem goes largely unattended and unsolved.

Some 12,000 people are murdered with handguns every year in the United States. Yet the American people evidently have chosen to accept this loss of innocent life rather than pay the political and social cost of eliminating its cause.

Meanwhile, the U.S. government has expended hundreds of billions of dollars—and some 20,000 battle casualties in the Middle East—on the Global War on Terror, although only a few thousand American lives have been lost to terrorist attacks in the past 20 years.

The infamous al Qaeda attacks of September 11, 2001, took nearly 3,000 lives and destroyed tens of billions of dollars of property. In the wake of Hurricane Katrina, the U.S. Army Corps of Engineers recently confessed that its failures of construction and management of flood control projects had cost over 1,000 lives and tens of billions of dollars of property losses.[24]

This is not to say that we should not be concerned about terrorist threats, or that we should not be concerned about natural disasters or medical errors or other risks to lives, health, and property. The problem is that we have not had a comprehensive political dialogue about how we, as people, feel about the broad variety of risks we face and the relative priority we prefer in investing limited resources in doing something about them. It is just this sort of collaborative public engagement in making decisions about the people's own security, which the hard paradigm ignores, that the soft paradigm demands.

Control

The hard security path has pursued perpetuation of a traditional military preoccupation with 'command and control,' even in the unorthodox environments of 'asymmetric warfare' and 'homeland security.' The results have been broadly and progressively dissatisfying, for two essential reasons.

The first is easiest to summarize and dismiss. The attempted application of martial command-and-control doctrines within the American homeland persistently—and some would say fortunately—collides with the constitutional, legal, and political realities of the U.S. system of federalism.

The second and more generic reason, noted serially above, is that over four decades of analytical study and empirical observation of modern complex systems—going back to the early system dynamics work of MIT professor Jay Forrester[25]—indicate that the more tightly controlled are the efforts to manage such systems, the more they tend to behave in ways managers and policymakers find "counterintuitive." Attempts to strengthen command and control of such unruly systems typically spawn ever more confounding "unintended consequences" and tend to drive the systems toward "overshoot and collapse."

The more realistic and promising alternative offered by the soft paradigm starts by recognizing that traditional military notions of command and control have very limited applicability to the conditions of homeland security in a federal, constitutional, and 'all-hazards' environment. Instead, the essential soft-path prescription for the craving for command and control is: Less is more.

Reinforcing hard-path thinking, the federal government's post mortems of the Katrina-Rita catastrophe lamented the glaring breakdowns, or sheer absence, of the sort of pristine command and control called for by such technocratic nostrums as the official National Response Plan, and demanded improvement.

But, among others, political scientist Charles Wise derived from his review of the tragedy's record a call, instead, for a more "adaptive management" approach.[26] As Longstaff wrote even before that calamity, "Increasing evidence indicates that an adaptive management strategy that acknowledges complexity and uncertainty is more effective than a rigid command and control strategy, particularly in organizations that must deal with unpredictable events such as natural disasters and terrorism."[27]

The 'how-to' of an alternative doctrine of such adaptive management, or what proponents such as Michael Lissack call "coherence,"[28] is not a green field but a subject that has been studied and elaborated by management scientists for over 15 years. Replacing outworn, increasingly brittle and counterproductive command-and-control practices with participatory, adaptive, coherent management and organizational designs does not require invention but application.

Rather, "*broader* application" would be more accurate. For it would be a singular mistake to assume that public agencies are incapable or novices in providing the sort of adaptive security and response management that the soft path prescribes. In fact, the experience, practices, and culture of the U.S. Coast Guard are well aligned to what is needed. As suggested by Admiral Thad Allen, who ultimately was called upon to play the lead role in coordinating the Katrina-Rita disaster response:

> In my opinion, the operational genius of the Coast Guard is still that we give our field commanders a mission, an area of responsibility, and their own resources and assets, such as cutters and aircraft, and then we leave it up to them…. How much independent authority did I have to organize the mission when that was really a state and local government responsibility? So we had to negotiate everything…. If I had come in as the principal federal official and insisted on absolute unity of command … I felt it would actually have impeded some good work that had been started. So I elected to go for unity of effort instead.[29]

Participation

The flip side of 'softening' the ethos of command and control is broadening the scope and effectiveness of participation in preparing for and responding to critical conditions.

At least since the shift from conscription to an all-volunteer, 'professional' military in the 1970s, the hard path has furthered a view of national security as the job of a fairly limited elite of expert professionals, rather than of the broad citizenry or population as a whole. Some argue, in addition, that the Clinton administration compounded the effect by its replacement of the panoply of "civil defense" in favor of professional emergency response, through its revamped architecture of the Federal Emergency Management Agency (FEMA).[30]

In any case, the trend in the hard paradigm has been to disengage the American people from active participation in their own security.

On the opposite path, the soft paradigm propounds a view of national security as a shared responsibility of all members of society, renewing the civil defense tradition of broad, *active* public preparedness and participation. “Active” is a key concept and it underscores the practical difference between the hard and soft paths, particularly in the ‘homeland security’ domain. The latter distinction is exposed by the hard paradigm’s common reliance on the erroneous use of two key terms: “first responder” and “panic.”

“It’s critical that we readjust our thinking,” says hazards researcher Kathleen Tierney at the University of Colorado. “If you look at the 9/11 commission they talked about first responders versus what they called 'civilians,' as if all of the civilians did was just stand at the sidelines…. That is so radically at variance with what actually happened that day.”[31]

Representing the soft-path alternative, Dr. Mark Kirk, Assistant Professor of Emergency Medicine at the University of Virginia School of Medicine calls instead for “evidence-based” emergency planning based on “what people are *likely* to do, not what they *should* do.” [32]

There are few more acute indicators of the hard path’s root disinterest in an evidence-based understanding of human society than in its expressed determination to exercise bureaucratic control in order to prevent panic. One of countless examples is the federal government’s National Strategy for Pandemic Influenza, which includes the typical warning that “Effective risk communication is essential to inform the public and mitigate panic.”[33]

But Rutgers University professor Peter Sandman notes, “…panic prevention is the wrong goal—because it is relatively rare.” Actually, Sandman explains, “In moments of great danger, most people become preternaturally calm, not panicky.”[34]

Communication

The hard security paradigm’s view of the role of communications hinges on two key premises. First, consistent with the hard path’s notion that security is a job almost exclusively of a professional elite, largely to the exclusion of the general public, the focus of concern has been on the technology of communications within and among security agencies. Since 9/11 “interoperability” has been a major concern, based on the observation that the crazy quilt of different, incompatible radios and other communication systems among police, fire, and other agencies in multiple jurisdictions impaired their ability to work effectively together in a major crisis.

Second, because of the hard paradigm’s conception of the public as passive pawns in a bureaucratic chess game, compounded by its obsession with secrecy and sequestration of information, the hard paradigm’s approach to “risk communication” tends to be parsimonious and technocratic, based on a “one-to-many” model. This is typified by the prescription for risk communication in the aforementioned federal strategy for pandemic flu: “Ensure that timely, clear, coordinated messages are delivered to the American public from trained spokespersons at all levels of government….”[35]

In these regards, the hard paradigm is out of touch not only with expert knowledge about how effective risk-related communication works, but with the real social-technical environment of the modern world of the ‘blogosphere,’ MySpace, YouTube, open source software, SMS, IM, ubiquitous personal/mobile text/audio/visual communicators, and so on.

The Holy Grail of interoperable, official communications technology, despite the investment of billions of dollars in the quest for a ubiquitous technical fix, remains as elusive as the legendary totem itself. Like the similarly unattainable fix for “information sharing and collaboration,” a solution is obstructed by the hard path’s characteristic opacity to human factors and social reality—in this case, as Mark Kirk among others[36] emphasizes, that the reality is that collaborative communications depend, first and foremost, on *trusted relationships* among persons and organizations.

Effective risk communication with and among, as opposed to just ‘at,’ the public is even more dependent on trust, as Paul Slovic observes:

> The limited effectiveness of risk-communication efforts can be attributed to the lack of trust. If you trust the risk manager, communication is relatively easy. If trust is lacking, no form or process of communication will be satisfactory.[37]

Longstaff observes, additionally, that people generally meet the critical need for trustworthy information sources under conditions of risk and uncertainty by turning to persons with whom they already have a trusted relationship.[38]

The significance of these findings is compounded by the fact that public trust or confidence in government institutions—indeed in formal institutions broadly—is generally no more than moderate to low. In a 2006 Harris poll,[39] for instance, the institution which received the highest share of the public expressing “a great deal of confidence” was the military, but that was only 47 percent in February of 2006, down from 71 percent four years earlier. Only 25 percent of the public expressed a great deal of confidence in the White House, which was still a little better than the 14 percent who had great confidence in the press and only 10 percent who felt a high level of trust in Congress.

And the trend in confidence or trust in all institutions has been downhill for several years. A worldwide survey for the World Economic Forum’s meeting in December 2005 showed a similar pattern: 9 percent *more* people said they *don’t* trust than do trust national governments “to operate in the best interests of our society,” while 29 percent more people said they *do* trust than don’t trust non-governmental organizations (NGOs).[40]

The soft paradigm would correct these distortions and weaknesses in security communications by shifting to a person-to-person and many-to-many model. Rather than limiting communication to an official elite, the soft path extends the perimeter of the engaged community to embrace all stakeholders, participants, and interested parties among public agencies, private organizations, and the general public. And instead of dictatorial edicts emanating one way from the center to the periphery, and scrubbed through professional spin-masters, the soft path nurtures multidirectional conversations around and through multi-path webs.

Technology

The hard-soft cleavage in the design and use of technology was crisply illuminated in a bellwether book over 20 years ago by Shoshana Zuboff, then a professor at the Harvard Business School. Zuboff began that volume, *In the Age of the Smart Machine,* by illustrating the typically counterproductive consequences of the hard engineering paradigm with the case of a paper mill she had studied in depth.[41]

Zuboff zeroed in on the design of the doors to one of the mill's control rooms, which required operators to wait for one set of automated glass doors to open and close, wait in an airlock, and then wait for a second set of automated doors to let them pass in or out.

The seemingly rational design turned out to be utterly, and dangerously, incompatible with real human behavior. Instead of waiting for the automated outer door to function, Zuboff observed that the plant workers "force their fingertips through the rubber seal down the middle of the outer door and, with a mighty heft of their shoulders, pry open the seam and wrench the door apart." After three years of the workers forcing the mechanism hour after hour, "the door is crippled."[42]

One might think that, in over two decades since Zuboff's critique, the design and management of technology projects would have learned from such negative experiences and become more sensitive to human factors and organizational cultures. One might also think that when national security is concerned, in light of the high stakes, the need to understand the nuances of human and social requirements and to adapt technical designs accordingly would be addressed even more urgently.

One might be surprised, and disappointed.

True, in the private sector there has been some palpable advancement in artful designs that cannily harmonize technical architectures with social demands. But, despite some opening of government markets to commercial off-the-shelf (COTS) solutions, the amalgam of bureaucratic gridlock, opportunistic contracting, and pork-barrel politics has left government often lagging, sometimes acutely.

Salient to this discussion is the glaring example of the Federal Bureau of Investigation's Virtual Case File (VCF) project, which *IEEE Spectrum* characterized as "the most highly publicized software failure in history."[43] The VCF was one of the major repercussions, and urgently demanded remedies, stemming from the disastrous attacks of September 11, 2001. It was evident only shortly after the tragedy that the FBI's archaic information systems were a key contributing factor.

The VCF was supposed to be the technical fix. Yet when FBI Director Robert Mueller attempted to run a demonstration of the new VCF at a press briefing in the Bureau's command center in early 2003, the system ominously crashed.[44]

By 2005, having spent $170 million, the FBI found that the 700,000 lines of code its contractor, Science Applications International Corp. (SAIC), had delivered were "so bug-ridden and functionally off target that…the bureau had to scrap [the entire] project, including $105 million worth of unusable code." While the FBI initially blamed SAIC for the fiasco, several government and other studies showed that the bureau shared much of the responsibility for the project's mismanagement.[45] Blame was not in short supply.

As is typical of the sort of hard-path technology bungles that Charles Perrow once labeled "normal accidents,"[46] *Spectrum*'s investigation found that there had been "an early warning from one member of the development team that questioned the FBI's technical expertise, SAIC's management practices, and the competence of both organizations."[47] And the response to that warning was typical of the hard paradigm's uniquely dynamic constipation when 'national security' is involved:

> Matthew Patton, a security expert working for SAIC, aired his objections to his supervisor in the fall of 2002. He then posted his concerns to a Web discussion board just before SAIC and the FBI agreed on a deeply flawed 800-page set of system requirements that doomed the project before a line of code was written. His reward: a visit from two FBI agents concerned that he had disclosed national security secrets on the Internet.[48]

In May 2004, the Bureau announced a new, four-year project, Sentinel, that would "do the VCF's job and provide the bureau with a Web-based case- and records-management system that incorporates commercial off-the-shelf software." In March 2006, the FBI awarded a new six-year, $305 million contract to defense contractor Lockheed Martin to carry out the Sentinel overhaul, aiming for completion in 2009. But Ken Orr, an IT systems architect and adviser to Director Mueller, remained skeptical. “The sheer fact that they made that kind of announcement about Sentinel,” said Orr, “shows that they really haven’t learned anything.”[49]

At the heart of this festering fiasco is the hard path’s inherent disconnect between expedient system engineering and the stern but messy contingencies of organizational culture and human nature:

> Some FBI officials say the VCF mess shows just how much the senior leadership tends to withhold bad news from Mueller. “He is so isolated and shielded,” says one FBI official. Bureau insiders point to the culture in which the director is “like God,” and where the higher one climbs the management ladder, the riskier it is for the “palace guard” to alienate the boss. “The top guys around him,” says this official, “there’s no way they were going to tell him the bad news because VCF, it was his baby, and no one was going to say, 'Your baby’s ugly.”[50]

The foibles of the VCF are not unique but typical of the U.S. government’s conventional, hard-path quest for technological ‘silver bullets’ to slay the terrorism beast—symptomatic of the hard paradigm’s endemic preference for prevention over adaptation, and resistance over resilience. In the area of aviation for instance, security consultant James Zumwalt observes that, while the U.S. focuses on costly technology to screen passengers and baggage for terrorist weapons, Israeli security focuses on behavioral analysis and training aviation personnel to identify terrorists.[51]

This and other examples[52] of the misdirected thrust of the hard paradigm’s investment in technical fixes are driven not only by technocratic tunnel vision, but by the confluence of political and proprietary interests that profit from such projects, even when they are fruitless or wasteful. “DHS is organized to serve contractors,” observes John Meenan, chief operating officer of the commercial airline association,[53] echoing Charles Perrow’s pithy observation that “Disasters are funding opportunities:”

> As soon as [DHS] was established, the corporate lobbying began.… A web page document, “Market Opportunities in Homeland Security,” introduces one to the “$100 billion” homeland security marketplace, for $500.00 plus shipping.[54]

But government contractors also are prone to having their behavior contaminated by technocratic distortions of organizational culture. Regarding VCF, David Kay, a former senior vice president of SAIC who later was chief U.S. weapons inspector in Iraq, admitted that “SAIC was at fault because of the usual contractor reluctance to tell the customer, ‘You’re screwed up. You don’t know what you’re doing.’”[55]

Official declarations of disaster areas and the federal funds that follow correlate with the priority of presidential political interests. Small states whose senior legislators occupy powerful committee positions of senior legislators have persistently tended to get a higher per-capita share of federal funding than populous and presumably high-risk states such as New York and California. So, again, "Disasters are funding opportunities."[56]

Note that much if not most of these lucrative funding opportunities involve the research, development, testing, demonstration, or acquisition of technical equipment and systems—often indifferently to the actual risks and needs faced by the acquiring organizations, or their ability to employ their new gadgets effectively.

One of many examples is this: The tiny town of Bellows Falls, VT, with just eight police officers, two chairs in the barbershop, and one screen in the local cinema, used federal grant money to acquire 16 video surveillance cameras—only three fewer than Washington, DC, whose population is 181 times greater.[57] In 2003, the number of murders and homicides in Bellows Falls was zero (a fictional murder did take place there in a 1998 novel by Archer Mayor); in Washington that year there were 248 murders. The relative risk of terrorist attack in Washington is presumably far greater.[58]

It is precisely because technology decisions are driven by forces that are not technical, and frequently not even evidently rational, that the hard paradigm's technology agenda is destined to yield only more such misadventures of costly failures and distorted investments.[59] The soft paradigm promises no panacea to the foibles of human nature, but at least offers the potential of better outcomes if only by dint of being more realistic.

In place of the hard path's technocratic tunnel vision, the soft paradigm aims at investing in *social*-technical innovation processes—building on the body of social, behavioral, cognitive, psychological, organizational, and other human-factors research knowledge. And the soft path points toward managing technology and tangible infrastructure not as autonomous 'assets' but as dependent elements of complex, socioeconomic systems.

The basic conception of human-centered technical design began with the discovery of the "learning curve" in the 1920s, and then serially evolved through the development of "sociotechnical system design" at the Tavistock Institute in the 1950s and, later, "total quality management" and "business process reengineering." Its current expression can be observed in the work of leading commercial design firms, which characteristically begin projects with exhaustive study of human and social factors before any technical designs are plotted.

One example is the Opti Desktop PC, which won a gold award for China's Lenovo Group and its American design partner ZIBA Design in *Business Week*'s latest annual industrial design competition. The design team, *Business Week* reported, "…spent months immersed in Chinese music, history, and objects of desire, such as cell phones, observing families as they lived, worked, and played."[60]

The potential benefits of applying this kind of human-centered design discipline to the problems of national/homeland security are boundless—arguably the more so for being, to date, so largely untapped. Achieving them will require a soft-paradigm shift in security strategy, one that gives the human sciences top priority in "science and technology."

Paradigm Shift: Implications for Critical Infrastructure Protection

How would a shift in security paradigms from the hard path to the soft path affect strategy for "critical infrastructure protection"?

First, it is the central notion of *critical* infrastructure, assets, and such that most sharply divides the hard and soft strategies for investing always limited resources to mitigate risk and improve security. Consistent with its orientation to assets, the hard paradigm aims to order the priority of security investments in accordance with the relative 'critical-ness'of infrastructure assets.

In a resilient society, 'critical infrastructure' is not better protected. Rather, in a resilient society there is less (ideally no) 'critical infrastructure' to protect. By way of illustration, the dilemma of 'asymmetric' warfare is that enemies are diffuse, dispersed, polycentric, interactive but minimally integrated, often invisible—and thus offer little or no 'critical infrastructure' to attack.

It follows that re-labeling government programs to replace "critical infrastructure *protection*" with "critical infrastructure *resilience*" does not solve this basic contradiction.

Moreover, investing in "critical" infrastructure, however broadly defined and whether the aim is protection or resilience, is inherently flawed by the near impossibility of knowing, in an astronomically complex global economy, what actually is "critical." For instance, a fire in a Sumitomo Chemical Co. factory in Japan in 1993 led to an acute worldwide shortage of computer chips for months afterward. The factory did not make computers or computer chips, but provided some 60 percent of the world supply of high-grade epoxy resin required to bond the plastic packages that hold integrated circuits.[61]

While computer chip factories may have the 'sex appeal' to make the list of what many politicians or bureaucrats might consider "critical," the dependency of that whole industry on a product as seemingly mundane as *glue* probably would not—and in fact did not—make the "critical" cut until after an acute disruption occurred.

With its more complex, ecosystem vision of infrastructure, the soft path leads toward a very different investment strategy, aimed at reducing the *brittleness* of systems and of the linkages among systems of systems. The soft paradigm thus seeks greater resilience *of the whole*, not just of what may be bureaucratically or politically deemed "critical" to certain limited interests.

The differences in the hard and soft strategies are illustrated by recent developments in the telephone industry. For over a century, the traditional telephone network has been dependent on centralized switches in central phone company offices. The brittleness of this architecture was demonstrated when an error in a single line of software crashed AT&T's long-distance telephone network for nine hours in January 1990.[62]

European upstart Skype, in contrast, has little or no central infrastructure to protect. Instead, Skype provides VoIP (Voice over Internet Protocol), peer-to-peer software that is distributed among some 200 million personal computers worldwide and that allows users to employ the resilient (albeit not impregnable) global Internet to make calls to other people anywhere either for free or for a nominal charge far less than that of the traditional phone companies.

In practice, making the soft-paradigm shift from the current, self-limiting quest for 'critical infrastructure protection' to a strategic doctrine of social resilience would require a few key steps:

1. Make *resilience* a ubiquitous standard of infrastructure design and management.

   Because we cannot know reliably what infrastructure is critical, and alternatively because all infrastructure is critical to some community, both public policy and private enterprise will benefit from raising the level of resilience of all infrastructure. Moreover, in an age of globalization, the standard of infrastructure resilience must be raised not just in the U.S. but internationally. Infrastructure management in this regard is on a par with environmental management or public health management, which are accepted as essential missions in every community.

2. Manage *risk* as a social/behavioral construct.

   Again, risk is about emotion not about mechanics. Risk management is not managing assets but managing human perceptions, feelings, and behaviors. Engineering analytics such as RAMCAP do not provide risk assessment, although they may contribute some useful information for risk assessment. In any case, strategic and operational decisionmaking must cope with uncertainty and surprise even more than with known risks.

3. Renew the ethos of *civil defense*; engage the 'wisdom of the crowd.'

   The complexity of modern security challenges—particularly those posed by catastrophic events—exceed the capacity of a limited cadre of expert professionals to anticipate or manage. The lessons learned from recent events—from counterinsurgency to law enforcement to disaster response and recovery—all underscore that the public as a whole will play an active role in any case, and should have its active participation formally engaged. Regarding infrastructure, it is widely recognized that the vast majority of infrastructure is privately owned and controlled, and hence subject to only limited government management. But improving broad, community-based decisionmaking about infrastructure design and development, as well as planning for disasters and recovery, requires curtailing the recent cult of secrecy about infrastructure risks so that private actors and citizens can make informed choices.

4. Apply the sciences of *human factors* to improve performance.

   Behavioral, social, cognitive, and other scientists already have accumulated a rich mine of knowledge about the human factors that lie at the heart of security threats and crisis responses. Further research investment certainly is needed to keep apace of fast-evolving trends in terrorist threats, global information architecture, economic infrastructure and processes, and so on. But a more critical (and largely unmet) need is to apply this knowledge effectively to improve the performance of official agents, organizations, and members of the general public in managing security problems. So-called 'lessons learned' archives are of little value if their contents are not scientifically validated and are not properly applied to 'evidence-based' strategy, planning, operational tactics, and training.

5. Take the long view.

   Because much infrastructure is durable, brittle infrastructure often cannot be immediately replaced or reconstructed, although mitigating measures and backup/redundancy options should be adopted to improve the resilience of the processes that depend on it. But infrastructure is continually turning over, so better standards for assessment and design adopted in the near term will lead to progressively more resilient systems over a period of decades.

Prospects

The diversity built into America's political, economic, and cultural systems is an innate, constitutional bias toward the adaptability and resilience that the soft security paradigm seeks to promote. Adaptation and resilience do not need to be invented so much as protected and reinforced.

Nevertheless, shifts in dominant social/political paradigms may not be swift and are not inevitable. Proponents of the soft paradigm need to be prepared for obstacles along their path.

One is obvious: the prodigious number of people, organizations, and interests that are powerfully and profitably invested in the national security status quo. The brouhaha that is chronically kicked up by any attempt to close a redundant military base, cancel a costly but obsolete weapons system, or deny a homeland security grant are all mundane evidence of the sort of well-heeled backlash that those who seek to change the direction of security strategies, and thus investments, can expect to provoke.

A second obstacle is less obvious but often more daunting than overt resistance: that is, co-optation. The tactics of "old wine in new bottles" are all too common precisely because they are so often effective in preserving the status quo in a wrapper of symbolic ‘innovation.’ It is easier and more likely for politicians, bureaucrats, and vendors to adopt the rhetoric of “adaptation” and “resilience” than to make substantive commitments of resources, people, and action to a functionally different strategic path.

Still, in the past half-century, our society has experienced dramatic changes. Smoking, once a ubiquitous social practice is now stigmatized and shunned. Formal racial segregation and discrimination has been replaced by a society which, if imperfect, is vastly more open, tolerant, and diverse. The role of women has been transformed. The Soviet ‘evil empire’ is gone. Environmental protection, initially viewed as a radical threat to free enterprise, is now largely embedded in business-as-usual.

So, while the outcome of the contest between hard and soft security paradigms remains to be seen, in the words of the late Kenneth Boulding, “Anything that exists must be possible.”

Hard vs. Soft Security Paradigms

	Hard	Soft
AKA	Prevention / Resistance	Adaptation / Resilience
Priority	substantially higher priority attached to terrorist threats than to other threats or risks	renewal of a balanced, ‘all-hazards’ consideration of threats or risks
Protection	‘hardening’ potential targets against any/every imaginable attack	‘softening’ the brittleness of potential targets by reducing their vulnerability profile through redundancy, lower cost, dispersal, reduced scale, self-healing, accelerated repair/recovery, and so on
Risk Concept	concept of ‘risk’ rooted in engineering	concept of ‘risk’ embracing social perceptions and public choice
Control	perpetuation of a traditional military preoccupation with ‘command and control’, even in the unorthodox environments of ‘asymmetrical warfare’ and ‘homeland security’; a view of national security as the job of a fairly limited elite of expert professionals, rather than of the broad citizenry or population as a whole	recognizing that traditional military notions of command and control have very limited applicability to the conditions of homeland security in a federal, constitutional, and ‘all-hazards’ environment; a view of national security as a shared responsibility of all members of American society, renewing the ‘civil defense’ tradition of broad, *active* public preparedness and participation
Communication	‘one to many’ model of public communications	‘many to many’ model of public communication
Technology	investment focused on a search for technical fixes that permit continuation of established economic, social, political, and/or organizational behavior and structures	investing in social-technical innovation processes—building on the body of social, behavioral, cognitive, psychological, organizational, and other human-factors research knowledge—while managing technology and tangible infrastructure as dependent elements of complex, socioeconomic systems
Strategy	strategy aligned toward ‘critical-ness’	strategy aligned toward ‘brittleness’

Acknowledgements

The author is grateful for suggestions and comments generously provided by Joel Arthur Barker, William Cumming (Vacation Lane Group), Dorothy Denning (Naval Postgraduate School), Baruch Fischhoff (Carnegie-Mellon University), Jeffrey Gaynor (Homeland Security Policy Institute), Ern Lewis (Environmental Tectonics Corp.), Britton Manasco (Market Intelligence Group), Michael Schrage (MIT Security Studies Program), Jim Souby (Oquirrh Institute), Kathleen Tierney (University of Colorado), and Bert Tussing (U.S. Army War College), as well as the guidance and assistance of Christine Pommerening (George Mason University). The views expressed here are the author's own, as are any errors.

Notes

[1] I offer this caveat about that labeling: Proponents of 'hard' approaches not uncommonly derogate 'soft' alternatives as weak, ineffective, disorderly, or even ridiculous. However, the hard/soft distinction has become common in the vernacular of many relevant fields of professional practice, as in discussions of "hard" and "soft" power (military/political), energy architectures, skills, sciences, management practices, organizational designs, system engineering, and so on. Since labels should not be barriers to useful strategic thinking and planning, alternate labels can and should be used if needed. In another essay several years ago, I invented the labels 'M Class' and 'B Class' to reduce that stereotypical prejudice (see Lewis J. Perelman, "The Hypercube: Organizing Intelligence in a Complex World," *Executive Update*, Business Intelligence Advisory Service, Cutter Consortium, 2001).

[2] Amory Lovins, "Energy Strategy: The Path Not Taken?" *Foreign Affairs*, v. 55, no. 1, (October 1976, pp. 65-96).

[3] Quoting from David Brower.

[4] Lovins, 1976, p. 88; emphasis is mine.

[5] In my own book, *The Global Mind* (New York: Mason/Charter, 1976), I used the framework of 'hardworld' and 'softworld' paradigms to untangle the seeming dilemma of "limits to growth." (Not coincidentally: Lovins and I had met and compared our early thoughts about the hard-soft distinction in 1974.) There are numerous other examples and contributions from other authors. For instance, in a 1993 article on paradigm shifts in operations research (OR), management professor John Brockelsby of the U. of Wellington, New Zealand, noted that "Undoubtedly, the biggest growth area in OR in the last twenty years has been in what has come to be known as 'Soft OR' or 'Soft Systems'." ["Methodological Complementarism or Separate Paradigm Development…," Australian J. of Management, 18, 2 (Dec. 1993).] Prof. Joseph Nye first introduced the notion of "soft power" in the 1980s and elaborated it in several succeeding publications, most recently in *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004). Defense analyst Thomas P.M. Barnett, evidently viewing Nye's prescription for 'soft power' as perhaps too soft, nevertheless has framed his own call for a paradigm shift in security strategy in a widely discussed book [*The Pentagon's New Map: War and Peace in the Twenty-First Century* (New York: G.P. Putnam's Sons, 2004)], a popular blog, and numerous other presentations. Barnett's paradigm shift distinguishes and would separate the roles of what he calls 'Leviathan' (kinetic military force) to win the war and 'Everything Else' to win the peace (pacification, civil affairs, reconstruction, humanitarian assistance, special operations/forces, winning hearts and minds, and such).

[6] For a brief overview, see http://www.state.gov/r/pa/ho/time/cwr/17601.htm.

[7] Office of the Inspector General, *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina*, OIG-06-32 (Washington, DC: U.S. Dept. of Homeland Security, March 2006).

[8] Jane Bullock, FEMA chief of staff during the Clinton Administration, told a reporter shortly after Katrina struck, "The federal system that was perfected in the '90s has been deconstructed," noting a report that the U.S. was spending $180 million annually to defend against natural hazards while spending $20 billion a year to counter terrorism. ["Storm Exposed Disarray at the Top," *The Washington Post* (Sept. 4, 2005).]

Patrick Roberts questions the belief that FEMA, during the Clinton Administration under the direction of James Lee Witt, had solidified an all-hazards program that had been allowed to deteriorate after George W. Bush became president—suggesting that FEMA in the 1990s may have shortchanged attention to terrorism or other national security threats in favor of a main focus on natural disasters. [Patrick S. Roberts, "FEMA After Katrina," *Policy Review* (June-July 2006).]

[9] Jack Hayes, Director, National Earthquake Hazard Reduction Program, National Institute of Standards and Technology, address to annual meeting of the Multidisciplinary Center for Earthquake Engineering Research in Arlington, VA, June 29, 2006. Notably, the leadership of MCEER announced at the same meeting that it had decided to rename the organization just MCEER and broaden its agenda to address 'multiple hazards' under the rubric of "Extreme Events."

[10] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: Norton, 2004).

[11] Such planning for uncertainty is explored at length in P.H. Longstaff, *Security, Resilience, and Communication in Unpredictable Environments Such as Terrorism, Natural Disasters, and Complex Technology* (Cambridge, MA: Program on Information Resources Policy, Center for Information Policy Research, Harvard University, November 2005).

[12] For instance, the Critical Infrastructure Task Force presentation of January 2006 lends itself to that interpretation even though it constructively speaks of *extending* the current national policy goal from "protection against intentional acts" to "resilience against all-hazards," rather than *replacing*. See: Critical Infrastructure Task Force, "Presentation to Homeland Security Advisory Council," January 10, 2006 (Washington, DC, U.S. Dept. of Homeland Security).

[13] The distinction here is admittedly stereotypical. The reference to "traditional" Western medicine is to acknowledge that, over the past few decades, the allopathic medical establishment has progressively opened to study, scientifically evaluate, and adopt or adapt to some of the practices or concepts of alternative disciplines.

[14] The potential folly of the government's existing asset-fixation is demonstrated by the public reaction to a report from the DHS Inspector General, *Progress in Developing the National Asset Database*, OIG-06-40 (Washington, DC: Dept. of Homeland Security, June 20, 2006). The OIG reported that the database of supposed critical infrastructure included "unusual or out-of-place" sites "whose criticality is not readily apparent" such as Old McDonald's Petting Zoo, the Amish Country Popcorn factory, the Mule Day Parade, the Sweetwater Flea Market, and an unspecified "Beach at End of Street." News media latched on to the seemingly ridiculous finding that the database listed 8,591 potential terrorist targets in Indiana—"more than New York (5,687) and more than twice as many as California (3,212), ranking the state as the most target-rich place in the nation." ["Come one, come all, join the terror target list," *The New York Times* (July 12, 2006).]

[15] See Charles Perrow, "Shrink the Targets," *IEEE Spectrum* (September 2006).

[16] Longstaff, op. cit.

[17] Peter Fairley, "The Unruly Power Grid," *IEEE Spectrum* (August 2004).

[18] A representative example is *Risk-Assessment Methodologies for Use in the Electric Utility Industry* (Version 09/09/05), Prepared by the Risk-Assessment Working Group of the North American Electric Reliability Council's Critical Infrastructure Protection Committee, available at http://www.esisac.com/library-assessments.htm. Even more to the point, Appendix B of the latter provides a summary of the Risk Analysis and Management Approach for Critical Asset Protection, or RAMCAP, methodology developed for DHS through a contract with the American Society of Mechanical Engineers, which has been pointedly criticized by leading social and behavioral scientists for its lack of accommodation of human factors. For example, reviewing the RAMCAP report, Prof. Baruch Fischhoff of Carnegie-Mellon University, at the time president-elect of the Society for Risk Analysis and a member of the DHS Homeland Security Science and Technology Advisory Committee, commented, "The core of my concerns is that the document ignores social science concerns that are essential to risk management, as well as developments in the social role of risk analysis."

[19] Lester B. Lave, "Suggestions for Improving DHS Assessment of R&D Priorities," working paper, July 24, 2005.

[20] "No Friend Left Behind: The public demands evacuation plans for people and pets," AARP Bulletin, May 2006.

[21] For instance, see David Ignatius, "Taste of the Future," *The Washington Post* (February 24, 2006); James Jay Carafano and Alane Kochems, "Security and the Sale of Port Facilities," Heritage Foundation Web-Memo #997 (February 22, 2006).

[22] Brookings Institution transcript of Chertoff remarks on June 1, 2006.

[23] "Anti-terror funding cut in D.C. and New York," *The Washington Post* (June 1, 2006; p. A01). Ridicule of the UASI allocations was further inflamed by the DHS Inspector General's report noted above [OIG-06-40 (June 20, 2006)] of egregious flaws in the National Asset Database, which is presumed to be used as a basis for such grant decisions. *The New York Times* quoted Sen. Charles Schumer (D, NY): "Now we know why the Homeland Security grant formula came out as wacky as it was…. This report is the smoking gun that thoroughly indicts the system." [*Times*, loc. cit. (July 12, 2006).] "That's what's discouraging about this list," noted Sen. Susan Collins (R, ME), chairman of the Senate Government Affairs and Homeland Security Committee, "It does not seem to represent true targets." [Transcript, *Scarborough Country*, MSNBC TV (July 12, 2006).]

[24] "Katrina Report Blames Levees," CBS News/Associated Press (June 1, 2006).

[25] Some useful samples would include Jay W. Forrester, "Counterintuitive Behavior of Social Systems," *Technology Review* (January 1971); Lawrence M. Fisher, "The Prophet of Unintended Consequences," *Strategy + Business* (Fall 2005).

[26] Charles R. Wise, "Organizing for Homeland Security after Katrina: Is Adaptive Management What's Missing?" *Public Administration Review* (May/June 2006).

[27] Longstaff, op. cit.

[28] For example, see Michael Lissack and Johan Roos, *The Next Common Sense: Mastering Corporate Complexity through Coherence* (London: Nicholas Brealey, 1999).

[29] "New Coast Guard chief discusses lessons learned from Katrina," *Government Executive, Daily Briefing* (June 2, 2006).

[30] For instance, Patrick Roberts, op. cit. For further details on FEMA's evolution, see: Richard Sylves and William R. Cumming, "FEMA's Path to Homeland Security: 1979-2003," *Journal of Homeland Security and Emergency Management*, 1, 2 (2004).

[31] "Are we the real first responders?" *Christian Science Monitor* (July 14, 2005).

[32] Mark Kirk presentation at "Engaging the Frontlines," 2006 Spring Research Symposium of the Institute for Infrastructure and Information Assurance, James Madison University, at the National Academy of Science, Washington, DC, May 12, 2006.

[33] Homeland Security Council, *National Strategy for Pandemic Influenza* (Washington, DC: Homeland Security Council, November 2005).

[34] Dr. Peter Sandman, "Beyond Panic Prevention: Addressing Emotion in Emergency Communication," *Emergency Risk Communication CDCynergy*, CD-ROM, (Atlanta, GA: Centers for Disease Control and Prevention, U.S. Dept. of Health and Human Services, February 2003); also available at http://www.psandman.com/articles/beyond.pdf.

[35] Homeland Security Council, op. cit.

[36] Mark Kirk, op. cit.; also Longstaff, op. cit.

[37] Paul Slovic, "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield" (Eugene, OR: Decision Research, September 7, 2000); earlier version published in *Risk Analysis*, vol. 19, no. 4, 1999.

[38] Longstaff, op. cit.

[39] February 7-14, 2006; N=1016 adults nationwide; MoE ± 3.

[40] "Trust in Governments, Corporations and Global Institutions Continues to Decline," Press Release (Geneva, Switzerland: World Economic Forum, December 15, 2005); cf. www.WEForum.org.

[41] Shoshana Zuboff, *In the Age of the Smart Machine* (New York: Basic Books, 1984).

[42] Ibid.

[43] Harry Goldstein, "Who Killed the Virtual Case File?" *IEEE Spectrum* (September 2005).

[44] Chitra Ragavan, "Fixing the FBI," *U.S. News* (March 28, 2005).

[45] Goldstein, op. cit.

[46] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (New York: Basic Books, 1984; also Princeton: Princeton University Press, 1999).

[47] Goldstein, op. cit.

[48] Ibid.

[49] "FBI grapples with out-of-date computers," C/NET News.com (July 14, 2006).
[50] Ragavan, op. cit.
[51] James G. Zumwalt, "Aviation security insecurity," *The Washington Times* (August 17, 2006).
[52] For instance, the Counter-MANPADS program; viz., "Protecting Commercial Airliners from Missiles," *Defence & Arms* (July 5, 2006).
[53] Private communication.
[54] Charles Perrow, "The Disaster after 9-11: The Department of Homeland Security and the Intelligence Reorganization," *Homeland Security Affairs*, vol. II, issue 1 (2006).
[55] "The FBI's Upgrade That Wasn't," *The Washington Post* (August 18, 2006).
[56] Perrow, op. cit.
[57] "Federal Grants Bring Surveillance Cameras to Small Towns," *The Washington Post* (January 19, 2006; p. A01).
[58] Numerous other examples of such ironies are noted in Veronique de Rugy, "Are We Ready for the Next 9/11? The sorry state—and stunning waste—of homeland security spending," *Reason* (March 2006).
[59] Viz., "DHS Terror Research Agency Struggling," *The Washington Post* (August 20, 2006).
[60] "The Best Product Design of 2006," *Business Week* (July 10, 2006).
[61] "Sumitomo epoxy resin plant gutted; IC firms scrambling; supplied 60% of the market," *Electronic News* (July 12, 1993).
[62] Philip Elmer-Dewitt, "Ghost in the Machine," *Time* (January 29, 1990).

Moving Beyond Critical Infrastructure Protection to Disaster Resilience.

Paula L. Scalingi

President
The Scalingi Group, LLC
Washington, DC

Overview

As Hurricane Katrina so clearly demonstrated, we have not learned how to manage extreme disasters—either natural or manmade. In certain respects, this is understandable. Over the last few decades, populations and the critical infrastructures and essential service providers to support their way of life have mushroomed to cover much of the United States. Many large cities and towns have merged to form megalopoleis that encompass hundreds of square miles and millions of people. Today these sprawling urban expanses are overlapping and relentlessly expanding. An example is the Mid-Atlantic corridor from above New York City in Connecticut through New Jersey, Pennsylvania, Maryland, and down beyond Richmond, Va., and including the District of Columbia. This explosion of growth has been accelerated by advancing information technologies that effectively have interlinked the physical and cyber infrastructures that underpin global, national, and local communities in a complex system of systems. Included in this vast intersecting set of networks are organizations that supply services and also are part of, or dependent upon, supply chains necessary for operations and business functions.

The emergency management plans of these public and private sector infrastructures and essential service providers are, at best, adequate to address localized incidents and events. However, these plans do not take into account disasters with extensive and prolonged impacts that may include destruction of critical components, systems and facilities, causing outages of weeks or months and shortages of personnel and expertise to restore critical services. This fact was underscored by the release in mid-June 2006 of a U.S. Department of Homeland Security (DHS) report on the sufficiency of disaster preparedness plans of states and major municipalities. The report found only a handful passed muster.[1] Commissioned in the wake of Hurricane Katrina, the Report did not address the effectiveness of the respective jurisdictions' capabilities to implement their plans.

The not unexpected results of the DHS report raises starkly the dilemma of how states and localities, with limited manpower, funds, and technical expertise can assess all-hazards vulnerabilities and identify readiness gaps. Beyond this, jurisdictions must take steps to develop the capabilities to protect, prevent, and mitigate potential damage from any number of possible scenarios, as well as respond, recover, and undertake long-term restoration when a major disaster strikes.

Hurricane Katrina was the nation's wake-up call. It called into question the approach that has emerged since September 11, 2001, and which has been the focus of U.S. national policy since that time. This approach rests on protection of physical critical assets from terrorist actions and preventing cyber attacks to *ensure* the security of infrastructures. In light of the devastation wrought by Katrina and the vulnerability of a good part of the nation to extreme disasters—hurricanes, major earthquakes, tsunamis, floods, wildfires, volcanic eruptions, ice storms—it is clear that comprehensive preparedness should be a primary goal, if not *the* overarching mission of U.S. homeland security. Looking beyond natural disasters to a terrorist detonation of a small nuclear devise in a city or a global pandemic, it is obvious that protection of critical infrastructures is only one element, albeit an important one, of a holistic approach to *assure* (as opposed to guarantee) that critical infrastructures, and more broadly, regions and nations, are as *resilient* as possible to withstand extreme disasters.

What Resilience Means

We live in an era of uncertainty and increasing vulnerability. In our electronic age of complex, interconnected infrastructures and open societies, protection from terrorists, natural disasters, systems failures, or other threats cannot be assured despite all the resources that may be poured into preventative, defensive, and offensive measures. Moreover, practitioners, policymakers, and researchers are only beginning to understand at a superficial level the many and multi-layered interdependencies among these entities and the vulnerabilities associated with them under various scenarios that can cause direct and indirect cascading affects, including regional paralysis with far-reaching economic and political consequences.

Because protection sooner or later will inevitably fail, the focus must be on cost-effective mitigation measures, damage control, and reconstitution.

This is an unpalatable fact that political leaders, the media, and much of the general public have not yet accepted. The focus is on making the nation secure (i.e., keeping bad things from happening) rather than on assuming they may happen and incorporating protection into a comprehensive preparedness approach to dealing with the unthinkable. Such an approach can be defined as resilience.

Interestingly, it has taken nearly five years after September 11, 2001 for resilience to be adopted as the term of choice by many in the all-hazards and security communities. There are variations of the definition of resilience, but they are consistent in that:

- *A resilient infrastructure is a component, system, or facility that is able to withstand damage or disruption, but if affected, can be readily and cost-effectively restored.*

Resilience in effect encompasses protection, prevention, deterrence, risk-based mitigation, response, recovery and longer-term restoration. Resilience also includes training, education, and research, development and application of solutions that operationalize these activities. Resilience, by its nature, takes infrastructure interdependencies into account and is based on assessed risk. Resilience can be measured, unlike protection, which is defensive in focus and begs the question—“how much is enough?”

In the same vein:

- *A resilient region is a municipality, community, state, or multi-jurisdiction area that is able to bounce back, i.e., reconstitute rapidly from a catastrophic event with limited damage to public safety and health, the economy, and national security.*

Critical infrastructure resilience and, more broadly, regional disaster resilience, requires a different way of thinking about preparing for and managing disasters, including terrorist attacks, that falls outside of traditional emergency and security plans. Achieving resilience requires a comprehensive, all-hazards, cross-sector, grass roots-to-national level, integrated approach. Put differently, it requires *horizontal and vertical* cooperation and coordination of key public-private- and non-profit stakeholders that have responsibilities or vested interests in improving regional preparedness.

This paper makes the case for why U.S. decision-makers need to move beyond the focus of the past four-plus years on stopping another September 11 attack by protecting infrastructure and begin to the lay the policy and technological foundation for a comprehensive preparedness approach that incorporates the concept of protection within the broader disaster resilience framework. The paper will:

- Examine the recent debate on protection versus resilience as a primary focus of U.S. homeland security policies and activities;
- Note the evolution of the concepts of critical infrastructure protection, infrastructure resilience, and disaster resilience;
- Explain why achieving resilience is the desired end-goal by looking at examples of regional and state initiatives that have embraced the concept, and lessons learned from a major interdependencies exercise and from Hurricane Katrina;
- Outline a national initiative centered on the work of The Infrastructure Security Partnership (TISP) to develop a high-level regional disaster resilience framework; and
- Address how the U.S. Department of Homeland Security (DHS) and other federal agencies, including the Department of Defense (DoD), could adopt resilience as a priority along with protection and partner with states, localities, and other regional key stakeholders to undertake a comprehensive preparedness approach that can meet the needs of the nation to effectively deal with all-hazards threats and disasters.

Looking Beyond Protection

Recently, there has been some measure of debate, chiefly confined at the national level among a few federal, non-profit and private sector organizations on terminology associated with assuring critical infrastructure and essential services in a significant disaster. This debate is largely a product of differing perceptions, competing bureaucratic interests, personalities, and politics. It reflects differing views of the security/law enforcement communities and the all-hazards community and whether the primary focus of homeland security should be on critical infrastructure protection or critical infrastructure resilience.

The bureaucratic stakes are fairly high, particularly for those within DHS that are managing resources and programs within the current organizational structure. Despite recent reorganization and creation of the Preparedness Directorate, DHS still focuses primarily on protection from deliberate threats and incidents. On a political level, the federal focus on protection has led to expectations on the part of Congress, the media, and the general public that the U.S. Government has the responsibility to ensure the nation’s critical infrastructures are safe from attack and disruption. With the 2006 off-year elections, and the campaign for the 2008 presidential election ahead, political party leaders on both sides are placing infrastructure protection high on their list of campaign priorities.

At the same time, the term infrastructure resilience or disaster resilience has become increasingly used within the academic and non-profit communities, as well as by officials at the state and local level who are involved in regional preparedness planning and public-private partnerships. DHS's Homeland Security's Advisory Council (HSAC) in January 2006 produced a report calling for the adoption of critical infrastructure resilience (CIR) in lieu of CIP, as the "top-level strategic objective—the desired outcome—to drive national policy and planning."[2] The Infrastructure Security Partnership (TISP), a national forum of the engineering and built environment communities, established a cross-sector task force in November 2005, which produced in June 2006 for practitioners a strategy for comprehensive preparedness—*Regional Disaster Resilience: A Guide for Developing an Action Plan*.[3]

This focus on resilience has elicited concerns, as previously noted, on the part of some senior officials within the federal government with defense, law enforcement, and security backgrounds that see the refocusing on resilience as redirecting the nation away from focusing on the terrorist threat. DHS and other related federal agency programs have centered on physical and cyber security preventive measures. A central element has been raising awareness of threats and vulnerabilities and collecting information on them through developing relationships and information sharing arrangements with specific companies and private sector organizations comprising identified "sectors." The conceptual design for this policy thrust based on protection has been embodied in DHS's National Infrastructure Protection Plan (NIPP), a weighty, dense, acronym-peppered treatise of more than 200 pages largely focused on protection of "critical infrastructure and key resources" (CI/KR).[4]

There are fundamental problems with the sector approach and national security focus of the NIPP:

- The overall focus on terrorism and infrastructure protection to "prevent, deter, neutralize, or mitigate" efforts by terrorists "to destroy, incapacitate, or exploit the Nation's CI/KR"[5]
- An implicit assumption that what would be useful to DHS and Sector-Specific Agencies (federal departments or agencies that have regulatory roles or leads for particular infrastructures) applies to the nation's extensive, diverse, and complex, interdependent private and public infrastructures and organizations. This is not the case with these organizations, most of which are privately owned, not subject to federal oversight and direction, have a regional customer focus and disaster preparedness orientation, and see non-manmade threats as the highest priority. Most major utilities fall into this category, as do states and localities. For

these organizations, national security rarely is an interest and is not a priority. Those that may focus on national security concerns do so because they have a significant federal customer base or are subject to legal or regulatory requirements. An example would be telecommunications providers or certain defense contractors deemed critical to the U.S. Government for mission assurance.

- Although there is a reference to the importance to regional cooperation, there is no real appreciation that disasters must be dealt with at the regional level. Nor is there recognition of the extent to which utilities, municipalities, counties, states, and multi-state regions at the grass-roots level have set up a wide variety of cooperative, often overlapping mechanisms to improve regional preparedness. These "partnerships," range from infrastructure security and other homeland security-oriented coordination groups and committees, law enforcement-focused mechanisms, community groups, regional public-private partnerships, and other types of networks, some technology development-focused. At the same time, in some parts of the nation at the regional level, utilities are increasingly collaborating with their regional sector competitors to address backup, response, and restoration needs in disruption scenarios. For example, in the Pacific Northwest, the Bonneville Power Administration is leading a collaborative effort of regional power providers focused on mutual assistance. In a similar vein, Washington State water systems, through the Washington Water Utility Council, are developing a mutual aid program.

Most recently, DHS, responding to the post-Katrina environment to address disaster preparedness and to pressure from its HSAC and other organizations promoting resilience, has attempted to reframe the concept of protection to incorporate response and restoration.

Evolving and Converging Terminology

One can argue that there really is no issue here at all and that it is a question of semantics and what this terminology means to certain constituencies. Ironically, practitioners, experts, and decision-makers alike have come to recognize that our understanding of how to assure critical infrastructures and essential services is dynamic and evolving. The all-hazards community has been focusing for decades on *mitigation* of damages to infrastructures, developing plans and procedures, assessing vulnerabilities, hardening systems, building in redundancies, etc., and developing standards, policies, and technologies for this purpose. A prime example is the Federal Emergency Management Agency's (FEMA) Project Impact Program of the 1990s, which focused on assessing potential impacts to infrastructures from natural disasters.[6] There are, however, a host of other environmental and health and safety government programs, as well as industry and non-profit activities that focus on these priorities. Other programs and activities have focused on *disaster preparedness* or *readiness.* From the 1950s to the end of the Cold War, *civil defense* focused on preparedness for nuclear attacks and major disasters.[7]

Other government and private sector programs for years have centered on *infrastructure assurance* or its two elements, *security* and *reliability*. A particular concern was *energy assurance* in the mid-to-late 1990s with several large-scale regional electric power disruptions on the West Coast, in the Midwest, New England, and South, culminating in the so-called California energy crisis.[8] The August 14, 2003 power outage that blacked out much of northeast North America and part of the central U.S. raised energy assurance once again as a major priority challenge. For the DoD, an escalating concern through the 1990s was *information assurance*, particularly in the battlefield, where reliance on information systems for situational awareness is imperative. Other related DoD objectives that emerged as priorities during the 1990s were *force protection* and *mission assurance.* Most recently, DoD has added *installation protection* as a major focus area.

Legacy of the President's Commission on Critical Infrastructure Protection

The term *critical infrastructure protection* entered into the federal policy lexicon in the mid-1990s with the creation of the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1996. Funded with DoD dollars, the major impetus was increasing concern about terrorism, particularly threats to cyber systems. The Commission's composition was unique in that the Commissioners were for the most part mid-level federal managers with security, law enforcement, defense, or intelligence backgrounds. While half the Commission was envisioned to be comprised of private sector senior officials from the eight infrastructures studied, by the end of the Commission's work, only four were represented.

Although the mandate of the Commission was to focus on deliberate threats to infrastructures, the prevalent view within the Commission was that physical threats were well understood, unlike the emerging threat emanating from cyberspace. The Commission Report issued in October 1997 stressed "the importance of developing approaches to protection of our infrastructures against cyber threats *before* they materialize and produce damage to systems." [9]

The Report, despite the protection orientation of its charter and of several of its more prominent members, foreshadowed today's debate over protection versus resilience in that the authors used the terms infrastructure protection and infrastructure assurance interchangeably. Interestingly, the definitions at the end of the Report clearly defined infrastructure protection to be "(*p)roactive risk management actions intended to prevent a threat from attempting to or succeeding at destroying or incapacitating critical infrastructures. For instance, threat deterrence and vulnerability defense."*

The Report defined infrastructure assurance as "(*p)reparatory and reactive risk management action intended to increase confidence that a critical infrastructure's performance level will continue to meet customer expectations despite incurring threat-inflicted damage. For instance, incident mitigation, incident response, and service restoration."*[10] These definitions reflected the desire of the Report's authors to distinguish between protective ("proactive") measures narrowly delineated to be preventative measures, in contrast to assurance ("reactive") measures.

In reality, the term *assurance* in the body of the report was used to mean security and reliability *and* to include preventative measures. The definitions also demonstrate that the Commissioners and technical staff had different perspectives and were grappling with how to address emerging deliberate threats to infrastructures in the context of traditional all-hazards threats, which many of their agencies had roles and missions to address. As a result, for the most part, the term infrastructure assurance was predominantly used throughout the report, and the proposed organizational structure recommended for establishment by the President to meet the infrastructure protection challenge at the national level was called the "National Structure for Infrastructure Assurance." [11]

Since the publication of the PCCIP Report through the issuance of the Clinton Administration's Presidential Decision Directive (PDD) 63 in May 1998, and the Bush Administration's Homeland Security Presidential Directives (HSPD) 7 and 8, the term critical infrastructure protection evolved and took on differing scope and focus.[13] HSPD-7 established a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attacks," while HSPD-8 established "policies to strengthen the preparedness of the nation to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies..." Moreover, from 1998 through September 11, 2001, CIP came to mean for most individuals cyber security, as this was the predominant focus of officials within the National Security Council, led by then National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism Richard Clarke, along with DoD. After the September 11 attacks, the focus turned to physical protection, with cyber threats a secondary focus.

The creation and orientation of DHS institutionalized this focus on thwarting and deterring terrorist attacks. The incorporation of FEMA into the new DHS, and the migration to DHS of much of the "sector lead" federal agency infrastructure assurance mitigation missions solidified the focus on protection. The DHS directorate that was the focal point for a range of infrastructure protection responsibilities and programs, including the homeland security intelligence mission, was called the Information Analysis and Infrastructure Protection Directorate (IAIP). IAIP was populated predominantly with law enforcement, security, defense, and intelligence personnel. Much of the programmatic work centered on outreach to individual infrastructure sectors—to utilities and companies, as well as to the national level sector-focused Information Sharing and Analysis Centers (ISACs). The objectives of these programs was to collect and assess threat information and develop policies, methodologies, and technologies to uncover and assess vulnerabilities, improve security, and prevent or deter attacks. Outreach to states and major municipalities focused on identifying and collecting information on CI/KR that were perceived to necessitate protecting. Federal funds to states and localities for emergency preparedness diminished, and the influence and activities of the FEMA regions declined significantly. Federal funding conversely was increased for terrorist-focused grants through various programs, in particular the Urban Areas Security Initiative (UASI) process that was administered by the Office of Domestic Preparedness, a former Justice Department element incorporated into DHS.

That a significant attack or disaster could occur that could damage or destroy interconnected infrastructures with large-scale damage to health and human safety and regional economies was acknowledged but not a programmatic priority at the federal level. DHS senior officials regularly spoke of the need for public-private partnering for critical infrastructure protection, but cross-sector regional issues and developing regional strategies were largely relegated to sometime in the indefinite future. In the final draft version of the NIPP, interdependencies and associated regional preparedness activities were referenced but not meaningfully addressed.

Meanwhile, at the state and local level, and for private sector organizations, continuity of operations remained a traditional top priority. Increasingly, outside of Washington D.C., there was interest in looking at the vulnerabilities associated with internal and external organizational and regional linkages among critical infrastructures and essential service providers. Collaborative mechanisms emerged in major municipalities and at the state level in different regions of the country and in Canada. These partnerships brought together representatives at the working level from emergency management, security, operations, and other disciplines from government and private sector entities, non-profits, businesses, and academe. The objective was to look at preparedness improvements to withstand terrorism, and particularly natural disasters with a focus on mitigation, response, and recovery activities that could improve readiness and lessen impacts.

Logic of Resilience as a U.S. Priority

As previously noted, resilience refers to the capability to prevent or protect against significant, all-hazards threats and incidents, including terrorist attacks, and to expeditiously recover and restore critical service if the unthinkable happens. Resilience, in sum, is very much synonymous with comprehensive preparedness. Resilience *includes* protection and prevention, which are important elements of it. Resilience is proactive and implies strengthening facilities, systems, and communities. Resilience by its nature takes into account interdependencies among infrastructures, including suppliers and customers. It necessitates a regional, cross-jurisdiction, integrated horizontal and vertical (grassroots to federal) approach to address these interdepenendencies, identify preparedness gaps, and develop/implement risk-based solutions. Unlike the term "resistant," which like protection implies that one can keep disaster from striking, resilience assumes that, on occasion, major emergencies will happen, the best course of action is to take protective measures where cost-effective while at the same time to be well-prepared to respond, recover, and restore infrastructure and resume operations expeditiously when necessary.

Grassroots Initiatives focused on Regional Resilience

As noted, since the September 11 attacks, there have been a growing number of regional and cross-sector cooperative initiatives focused on resilience. Some initiatives have been started by business groups, others by local or state government officials, while still others were founded by economic development associations or other non-profit entities. Some of the more productive ones have focused on regional infrastructure interdependencies. These initiatives are unique in that they include many of the "key stakeholder" organizations in a region that have responsibilities for essential services and/or a significant vested interest in regional disaster resilience. They include utilities, commercial businesses (manufacturing, agriculture and food industries, information technology services companies, and defense contractors, as well as associations that represent different business interests), nonprofits, community institutions (schools and churches, academic institutions), and numerous local and state government agencies and regional federal facilities (civilian and defense installations). The first responder and law enforcement communities are actively involved, and, in some cases, local and state political officials.

Examples of these interdependencies-focused regional collaborative initiatives are in the Pacific Northwest (the five U.S. state and three Canadian jurisdiction Pacific Northwest Partnership for Regional Infrastructure Security, and the Puget Sound Partnership for Regional Infrastructure Security); the Midwest (consisting of the Iowa Partnership for Homeland Security, the Southeast Wisconsin Homeland Security Partnership, and the Great Lakes Partnership for Infrastructure Security and Business Continuity encompassing the Chicago metropolitan area); the Gulf Coast region (New Orleans and Louisiana); and the Mid-Atlantic (just beginning in Maryland). Some, such as the Puget Sound (soon to be Washington State) Partnership for Regional Infrastructure Security, the Iowa Partnership, and the Great Lakes Partnership are well-organized with solid local and/or state government support, while others are struggling to gain focus or momentum. Some have held major interdependencies tabletop exercises and developed action plans to address lessons learned from the exercises.[13] Two of these efforts (in Washington state and Louisiana) have resulted in the creation of regional cyber coordination groups to address cyber security, communications, and critical information infrastructure resilience needs after holding interdependencies exercises with scenarios including major cyber attacks with regional disruptions. The former is the Puget Sound Alliance for Cyber Security (PSACS) and the latter is the Louisiana group called the Southeast Cyber Anti-Terrorism and Security (SECATS). Both groups are developing action plans and have created regional portals, with DHS/US-CERT assistance, within the US-CERT website to share information and gain knowledge on threats and incidents.

Hypothetical Case Study for Resilience: Blue Cascades III

An example of a regional infrastructure interdependencies tabletop exercise is Blue Cascades III. This exercise is the latest of the cross-border, multi-state Blue Cascades series, which have focused on the coastal Pacific Northwest region and produced a wealth of information on high-level interdependencies-related vulnerabilities and preparedness gaps. While the first two Blue Cascades exercises focused on physical and cyber attacks and cascading impacts, Blue Cascades III, held in March 2006 in Bellevue, Washington, centered on an extreme disaster scenario of a 9.0 magnitude subduction zone earthquake. The more than 330 representatives from 150 organizations participating in the intensive two-day event produced hundreds of pages of written observations on lessons learned and recommendations for remedial activities that resulted in more than one hundred findings and seventy-four recommendations. The more than four dozen organizations involved in designing the scenario on the Pacific Northwest's equivalent to Hurricane Katrina developed the exercise to explore, identify, and assess what needed to be done to make the region as resilient as possible to a major earthquake. The exercise was unique in that it covered all phases of the disaster—prevention, protection, mitigation, response, recovery and particularly longer-term restoration (rarely a focus of preparedness exercises).[14]

Lessons learned from the exercise fell into a dozen overlapping categories. Some of the highlights included:

- Lack of understanding and information on the effects on facilities, operational, and business systems of a large magnitude earthquake, including cascading and simultaneous infrastructure failures and physical destruction of critical assets that could paralyze parts of the region for weeks or months;
- Failure to appreciate the task of rescuing thousands of individuals injured or trapped in buildings, the need to shelter or resettle tens of thousands of others, and attending to the dead;
- Lack of appreciation that damage and disruption of telecommunications and critical information assets would leave much of the region without telecommunications, emergency communications, and business systems;
- Need for "situational awareness"—knowledge of what is happening throughout the region as the disaster unfolded to enable optimal decision-making;
- Little knowledge of what state and federal agencies had to offer regarding assistance to respond to loss or damage to operational or business systems;
- Limited coordination of local and state government disaster preparedness plans and contingency plans of private sector organizations for a major disaster;
- Need for inclusion of private sector and other non-government organizations in regional preparedness planning with states and municipalities;
- Need to include regional/national defense assets in regional preparedness planning for a major disaster;
- Cross-sector information sharing is vital to disaster preparedness and management;
- Lack of clarity on how the state, localities, and federal government would interface in an extreme disaster where lines of authority were blurred, and officials in charge were unavailable or unreachable to make decisions on deploying/managing personnel and other resources;

- Absence of an evacuation plan that could move large numbers of individuals from homes and businesses in a chaotic situation of transportation gridlock, no power, and limited communications;
- "People issues" must be taken into account on the basis that personnel are integral to the ability of an infrastructure or organization to function;
- Need for a certification process to enable emergency medical, utility maintenance and other stakeholder-essential personnel to have access to buildings and get past roadblocks;
- Limited recognition of the extent of recovery and restoration challenges, how long it would take to remove debris and to restore and rebuild structures and critical assets such as electric power transmission and distribution systems, and the legal and political challenges that need to be overcome;
- The necessity of the transportation infrastructure for restoration of critical infrastructure operations and other essential services;
- No system to manage the influx of volunteer aid, including identifying which organization would be in charge of determining which entities or jurisdictions needed these resources;
- Shortage of personnel needed for restoration activities, particularly construction workers and structural engineers to certify buildings, bridges, and tunnels as safe;
- Most businesses and community organizations with the exception of larger companies are rarely directly involved in local or regional preparedness planning;
- No logistic system to effect re-supply of basic living necessities, equipment, and other resources following a large-scale disaster;
- Need for public and media education on how a cascading disaster would disrupt basic services and impact health and safety, as well as on what government can or cannot do.[15]

Blue Cascades III, even more than its two predecessor exercises, clearly underscored the necessity to look at preparedness for and management of major disasters from any cause in a regional resilience context because of infrastructure interdependencies. The exercise also demonstrated that a significant amount of work needs to be done to prepare for extreme disasters—whether a hurricane, earthquake, or terrorist attack. These tasks include: assessing risk in terms of resilience, improving plans, and securing the resources necessary to develop new procedures; undertaking research on interdependencies impacts and finding ways to protect, prevent, and mitigate damage and cascading impacts through hardening structures and systems; building in redundancies, establishing backup systems, and conducting education and training to minimize casualties and damage. Such activities would clearly require public education and support of the media and political leaders to focus on developing regional resilience. Also, because of interdependencies, public and private critical infrastructures and essential service providers would need to develop, test, and train for their disaster response and business contingency plans with all other key stakeholders in the region rather than in isolation. [16]

Some Hurricane Katrina Lessons Learned

Hurricane Katrina definitively showed that a comprehensive preparedness or resilience approach is necessary to assure that communities are able to withstand any disaster, including extreme events. Katrina also underscored the need for states and major municipalities to build and nurture a broad-based collaboration of key stakeholders with roles and missions or significant vested interests in disaster preparedness and management in order to mitigate shortfalls identified in interdependencies exercises such as Blue Cascades III. Katrina also made clear the importance of federal encouragement, guidance, and support.

Communities in the Gulf states and particularly the New Orleans region were acutely aware of the devastation that a category 3 or 4 hurricane could create. FEMA, the U.S. Army Corps of Engineers, and officials from New Orleans and adjacent parishes conducted a five-day Hurricane Pam exercise in July of 2004. The New Orleans Office of Homeland Security and Public Safety and regional public and private sector stakeholders had partnered, with DHS support, to develop and conduct two regional interdependencies exercises in 2003 and 2004 focused on physical and cyber attacks, respectively, with the latter focusing on disruptions to hurricane preparedness. Although these and other exercises identified and documented important and extensive preparedness shortfalls, lack of funds and technical and personnel resources constrained efforts expeditiously to mount the activities necessary to develop and implement necessary mitigation measures.

A particularly good example is the impact of Katrina on telecommunications, emergency communications, and critical IT infrastructure. It was not a matter of disrupted infrastructures, either directly or due to power failures, or disruptions of interdependent infrastructures. In this case, infrastructure was destroyed or damaged. For a few individuals with Blackberries or other similar electronic devices or pagers, digital communications were possible. For most, however, communications capabilities were non-existent. Although the federal, state, and local government and private sector stakeholders were aware of the possibility of a prolonged loss of basic services, including communications, little to no work had been done to address this possibility.

Among the key lessons learned, which have been a priority for the 2006 hurricane season, is the need for communications and critical IT infrastructure resilience—emergency communications contingency plans for private and public sector organizations; backup systems to assure redundancy to deal with outages of phone, cell phone, and Internet access; alternate communications systems, including mobile capabilities and IT systems that provide greater use of high speed Internet voice and data; customer contact, hotline numbers, satellite phones, and text messaging. Also needed are ways to ensure that communications providers and other critical infrastructures can provide and receive information from the state emergency operations center to maintain situational awareness and assist in service restoration prioritization. Other basic needs include training of first responders and other essential personnel on federal, state, and local plans and procedures and use of equipment, such as satellite phones, as well as ways to transport essential equipment and supplies during a regional crisis situation.

A particularly important lesson learned is that there is a need for training on the vulnerabilities of telecommunications and critical information systems and what this means for creating the level, extent and duration of self-sufficiency necessary for organizations and communities in a major disaster. This knowledge then needs to be factored into continuity-of-operations and business plans to take into account interdependencies and related restoration needs in regional disruptions, including mitigation strategies, priorities, and service restoration sequencing. [17]

Creating a High-Level Strategy for Achieving Resilience

Increasingly, key stakeholders involved in these regional collaborative activities have been expressing the need to get beyond the discussions at conferences and workshops on vulnerabilities and preparedness shortfalls, and towards taking tangible actions. Regional stakeholders also want to move ahead to develop plans that are realistic, practical, and focused on local needs. There is little interest in the national and sector-based focus of the current federal CIP efforts, and a distrust of silver bullet technology fixes. Some of these practitioners and experts see the need for a proactive, comprehensive, regional approach that provides a flexible, dynamic, and comprehensive set of simple and clearly stated guidelines that can assist states, localities, and other key stakeholder organizations to select activities and projects they can undertake collectively and individually to improve disaster resilience. Such a set of guidelines would also enable these stakeholders to measure the utility of their existing plans and readiness activities and gauge progress made.

Guide for Developing Regional Disaster Resilience

The challenge to achieving this strategy was recently undertaken by TISP, a public-private cooperative organization created after the September 11, 2001 attacks. A Regional Disaster Resilience (RDR) Task Force of close to one hundred representatives from more than fifty key stakeholder organizations from across the country, including federal agencies, was created and convened in mid-November 2005 to develop a guide to produce a regional preparedness action plan. Published in mid-June 2006, the guide leveraged much of the lessons learned from regional interdependencies exercises, such as the Blue Cascade series, and lessons learned from past disasters to develop a regional approach that can ultimately lead to disaster resilience on a national scale.[18] The intent of the RDR Task Force was to create a flexible, dynamic high-level framework for use by all levels of government and key service providers to help improve regional preparedness to address all-hazards disasters with the goal of "sensibly securing interdependent critical infrastructures and achieving disaster resilience."

The document is essentially a high-level strategy and a baseline of identified, stakeholder-validated, prioritized regional preparedness needs and activities. These needs and activities are listed under 12 categories:

1. Awareness and understanding of interdependencies
2. Appreciation of cyber threats and incidents
3. Resilient interoperable communications and information systems
4. Risk assessment and mitigation
5. Cooperation and coordination
6. Roles and responsibilities
7. Response challenges
8. Recovery and restoration
9. Business continuity and continuity of operations
10. Logistics and supply chain management
11. Public information and risk communications
12. Exercises, training, and education.

TISP is currently working with the Pacific Northwest Economic Region and the Puget Sound Partnership for Regional Infrastructure Security to build a best practices and solutions database that will enable users of the *Guide* to have access to available plans, technologies, methodologies, and other tools that can be leveraged to keep costs low and maximize standardization across regions.

An important benefit of the document is that states and localities, as well as private sector and other organizations, can use it to gauge the comprehensiveness and utility of their plans and procedures and of the region as a whole. State and regional stakeholders will determine which activities to undertake based on existing capabilities, assessed risk, available resources, and incentives.

Importance of Regional Public-Private Partnering

One of the most important recommended actions in the *Guide*—and essential to implementation of any action plan developed— is the creation of a regional partnership mechanism to facilitate identification of interdependencies-related preparedness gaps and stakeholder validated activities and projects to address them. As Hurricane Katrina, other recent disasters, and regional interdependencies exercises have shown, federal, regional, state, and local organizations that have roles or vested interests in disaster preparedness and management must work together to make needed improvements. These diverse stakeholder organizations must focus beyond their own interests, fence lines, and jurisdictions to undertake new thinking, approaches, training, and exercises. This integrated and horizontal integration will require unprecedented cooperation among government agencies at all levels and with the private sector and other key stakeholders. The guide provides a model partnering process used successfully to launch and develop public-private regional collaborations. This multi-step process entails bringing together key stakeholders in a region together under the joint leadership of state or local government (e.g., homeland security or emergency management director) and a major commercial association (e.g., a regional chamber of commerce, economic or industry development association); developing and conducting an interactive infrastructure interdependencies workshop and regional exercise; and a prioritized "action plan" (i.e., a regional strategy) to address identified readiness shortfalls.[19]

Refocusing the Federal Government

DHS and other federal agencies are not well-organized or culturally inclined towards regional, cross-sector programs. These agencies, for example, the U.S. Departments of Energy, Transportation, Commerce, and the Environmental Protection Agency, have narrowly defined sector-specific regulatory missions focused on public safety. They share their sector responsibilities with DHS, deferring to DHS on the critical infrastructure protection aspects of the sector over which they have purview. Within DHS itself, numerous large components have often overlapping responsibilities for CIP issues, among them the Transportation Security

Administration, the Office of Infrastructure Protection, the Office of Cyber Security and Communications, FEMA, and the Science and Technology Directorate. Within these large entities are a host of smaller components that focus on a “piece” of the overall disaster resilience challenge--sector outreach, exercises, infrastructure protection technology development, and state and local government issues.

These bureaucratic silos, intent on advancing their programmatic interests and prerogatives, have limited progress towards “jointness” within DHS or moving beyond the hierarchical, top-down culture to work collaboratively with states, localities, and private sector service providers. Recently developed federal plans, including the National Response Plan (NRP), with its sector-focused Emergency Support Functions, the National Infrastructure Protection Plan (NIPP), and the National Incident Management System (NIMS), reflect the difficulty of the federal government to recognize the diversity and interconnectedness among the multitudinous private and public organizations that comprise the universe of today’s critical infrastructures and essential service providers. These plans also reveal a lack of appreciation of the limited role of the federal government in assuring the protection and resiliency of the nation’s critical infrastructures, which are for the most part privately owned and operated. In addition, these plans still largely reflect the policies of the past, such as the half-century old Stafford Act, which was developed in the pre-electronic era when populations were not concentrated in large overlapping municipalities with the tightly integrated infrastructures that exist today.[20]

Although the Stafford Act has been updated and the NRP has been developed since September 11, 2001, the assumption behind these national plans, which is incorporated into state plans, is that localities in a major disaster will exhaust their disaster management capabilities and turn to the state, which when overwhelmed will call on the federal government, which may trigger the use of U.S. defense assets to support civil authorities. As the response to Hurricane Katrina revealed, such an approach to dealing with extreme disasters in an interconnected age is a plan that may on paper look appealing but is not a viable strategy.

The goal should be for key stakeholders in a region to work together with all levels of government to develop a regional comprehensive preparedness plan that ensures regional resilience based on resilient communities that, in turn, rely on resilient critical infrastructures and essential service providers.

Need for Proactive Action

Achieving this goal will not be easy, but it is essential for the nation to come to grips with preparing for and managing extreme disasters, including terrorist attacks.

- Infrastructure protection, physical and cyber should remain a major priority, not just aimed at terrorist or insider threats and attacks, but focused on hardening systems, building in systems redundancy, and developing tools and technologies to prevent service disruption or damages to assets and systems. This is consistent with the overarching goal articulated in the NIPP.
- There needs to be a significant course correction within the federal government, led by DHS, to broaden the primary goal of the nation beyond protection to resilience with major resources—personnel and programs, reoriented to focus on the rest of the variables that are part of the resilience equation—risk-based incident mitigation, response, recovery and especially long-term restoration.

It is difficult to see how any decision-maker—government or industry—could not visit the New Orleans region today and see the grim evidence of a failure to assure disaster resilience—devastated communities, economic base decimated, wholesale depopulation of areas of the city, and miles of empty, gutted, derelict homes and businesses amid piles of debris, dust, vermin—and the occasional vintage FEMA trailer sheltering a hardy soul determined to rebuild amid the destruction. It is interesting to speculate if the disaster that struck New Orleans had been a terrorist attack with a small nuclear improvised device, would rebuilding and repopulating in the impacted areas, given real and psychological contamination concerns, be even an option?[21]

Challenges

The chief impediments to identifying preparedness shortfalls and cost-effective solutions that can lead to regional and national disaster resilience are for the most part “people problems:”

- Lack of awareness, especially among government, private sector, political leaders, and the media of why they need to think beyond the status quo of existing policies, laws, plans and paradigms and examine emerging challenges associated with extreme disasters of all kinds in an interconnected age;
- Over-emphasis on the terrorist threat driven by fear of another September 11 attack that has made protection and prevention the over-riding priority to keep “bad things from happening” to tens of thousands of subjectively-identified critical assets and facilities;

- Failure to recognize that major disasters from other causes, particularly natural disasters or pandemics, have a higher probability not only of occurring but causing substantially more damage to infrastructures and to public health and safety than most terrorist attacks;
- Managers and senior officials in stove-piped organizations that look at emergency preparedness and security only within their own fence lines and interests;
- Vested interest of federal government officials that prompt them to cling to objectives and strategies that have become outmoded as new knowledge and insights are changing the way practitioners and experts view how best to secure interdependent infrastructures to withstand all-hazards disasters;
- Proclivity of key regional stakeholders to believe the problem is too complex and overwhelming to tackle, or who take the "head-in-sand" approach, or who take steps to enhance readiness and then lose focus and momentum, particularly in the absence of strong local and state leadership and support:
- Reactive government and industry leaders who are reluctant or uninterested in providing the encouragement and top-down guidance/assistance to galvanize and focus regional stakeholders to take the initiative and sustain progress towards disaster resilience.

Solutions

The first step is recognizing that the "science" of understanding interdependent physical and cyber systems is dynamic and that expertise in this emerging "discipline" is growing rapidly at the same time advancing technologies are revealing new threats and potential solutions that need to be understood and addressed. This paper has demonstrated how the focus and terminology of what, at the moment, is called infrastructure *protection* has emerged from previous concepts and is evolving into *resilienc*e. Five years from now, based on our increasing knowledge base and political and international developments, this focus could well be different.

Thus, we need to put the semantic debate on protection versus resilience aside to focus on what is important to the nation and the communities that comprise it, and that is ensuring that critical infrastructures are both cost-effectively protected and resilient. This requires that programs and activities to develop policies, plans, procedures, methodologies, and technologies to meet critical infrastructure protection and resilience challenges must be flexible to accommodate changing needs and priorities. Establishing regional public-private partnerships is essential to identify shortfalls, validate and prioritize activities, and develop an action plan (regional strategy) to undertake individual/collaborative solutions

The federal government, civilian and defense, is crucial to protection and resilience in providing technical expertise and other assistance to identify preparedness shortfalls and develop effective plans, including regional preparedness strategies that address infrastructure interdependencies. The federal government can also provide seed money and technology solutions *where appropriate*, that can be leveraged to help jurisdictions implement these plans and develop the capabilities necessary to deal with extreme disasters.

- The *where appropriate* issue should not be used to keep the federal government from providing such assistance, which has often been the case. A recent DHS report on the overall low level of state and municipal preparedness planning begs the question of how these jurisdictions will improve their plans—let alone their capabilities—without the resources and expertise to accomplish this. Moreover, because achieving disaster resilience in an interconnected age requires grassroots to federal (vertical) cooperation and cross-sector regional (horizontal) collaboration, fostering regional partnerships will be essential.
- To address these challenges and make forward progress as outlined above, federal senior officials should actively consult with state and local government representatives, the private sector, and other stakeholders in a forum suited to this purpose to produce an assessment that answers these questions:
    - What types of activities associated with developing regional disaster resilience could benefit from federal support, and what would be the nature of this support? This could be guidance, technical expertise, leveraging existing government capabilities (tools, technologies, approaches, and systems), and using regions as test-beds for pilot projects.
    - What types of activities should states and localities typically take responsibility to address, and what resources would be necessary to accomplish these activities?
    - What types of assistance could private sector organizations and non-profits bring to the table?
    - What avenues could be utilized, or regional cooperative mechanisms or governance structures created, to enable "pooling" of funding steams from various government, the private sector, and other organizations, and enable ethical program implementation with effective program oversight of joint projects?

Importance of Federal Support

On this latter point, one of the most significant activities the federal government can undertake with states and regional key stakeholders is to encourage, and where useful, to provide guidance on establishing public-private partnerships and other collaborative mechanisms. Public-private partnerships are an essential tool to enable regions and the critical infrastructures located within them to achieve disaster resilience. Because of interdependencies, there must be some form of regional collaborative mechanism available to coordinate, identify linkages, and associated vulnerabilities, and undertake cooperative protection and mitigation measures.

Such partnerships cannot in themselves assure resilience. Public and private sector organizations lack resources, mandates, expertise, and cultural orientation to do this, but all have their respective roles in disaster preparedness and management. The federal government is necessary for funds, expertise, policies, regulations and standards (where necessary or desirable), and to provide leadership and encouragement as useful to maintain stakeholder motivation. Beyond this, the federal government must prepare with the regions for major disasters to be ready to assist when local and state capabilities are not able to handle or recover from a large-scale event.

In sum, the federal government has a crucial set of responsibilities in helping regions achieve disaster resilience, which in turn is dependent on public-private partnering. Only through such regional partnerships will key stakeholders have a venue to share information, build awareness, and provide the integrated vertical and horizontal approach necessary to both protect infrastructures and ensure disaster resilience.

Notes

1. "U.S. Report Faults Nation's Preparedness for Disaster," New York Times, June 17, 2006, p. 10A. See also U.S. Department of Homeland Security, Nationwide Plan Review Phase 2 Report, and June 16, 2006. The review covered 56 States and territories and 75 urban areas. Plan components were assessed on a scale of "sufficient," "partially sufficient," or "not sufficient" to manage a catastrophic event. The majority of components assessed fell into the "partially sufficient" category.
2. Report of the Critical Infrastructure Task Force, Homeland Security Advisory Council, January, 2006, p. ii. The Homeland Security Advisory Council (HSAC) provides advice and recommendations to the Secretary on matters related to homeland security. The Council is comprised of leaders from state and local government, first responder communities, the private sector, and academia.
3. Regional Disaster Resilience: A Guide for Developing An Action Plan, The Infrastructure Security Partnership (TISP), June 15, 2006, 44 pp.
4. See the National Infrastructure Protection Plan Base Plan, Revised Draft NIPP, v2.0, Department of Homeland Security, January, 2006, 218 pp.
5. Ibid., p. 1.
6. Eric Holdeman, the Director of Emergency Management for King County, WA., describes the Project Impact program in his post-Katrina op-ed, "Destroying FEMA," The Washington Post, , August 30, 2005; Page A17. There was a great deal of controversy surrounding the discontinuation of Project Impact by the current administration. For background on Project Impact see "Project Impact: Building A Disaster-Resistant Community," FEMA, November 22, 1999, Release Number: 1293-71.
7. There are a number of policy experts and academics, both old and new to the field, who are re-looking at civil defense as an alternative to infrastructure protection because it has a national security

connotation. For others, however, the term has too much of a "looking backwards" and reactive flavor rather than a term such as resilience which connotes proactivity.

8. See Report of the U.S. Department of Energy's Power Outage Study Team" March, 2000, 65 pp. including Appendices.
9. Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection, July, 1997, pp. 3 and 5. (The author of this article, then director of the Division and Information Sciences Division at Argonne National Laboratory, served as technical liaison and advisor to the Commission for its duration.)
10. Ibid, Appendix B, p. 2.
11. Ibid., p. 49. Interestingly, the Report clearly articulated the need "to forge a partnership among all the players—to achieve joint, integrated, and complementary action" to assurance infrastructures "in the interconnected, cyber-oriented world of today. See p. 45.
12. See Presidential Decision Directive-63, issued on May 22, 1998. Both Homeland Security Presidential Directive/HSPD-7 and Homeland Security Presidential Directive/HSPD-8 were issued on December 17, 2003.
13. In the past four years, there have been several regional interdependencies exercises modeled on the first exercise of this type, *Black Ice,* which was developed with regional stakeholders as part of the Salt Lake City 2002 Winter Olympics planning process. These exercises include *Blue Cascades I* (Portland, Oregon, 2002), *Golden Matrix (*San Diego, 2003), *Purple Crescent I (*New Orleans, 2003), *Amber Waves (*Des Moines, Iowa, 2004), *Blue Cascades II* (Seattle, 2004), *Purple Crescent II* (New Orleans, 2004), *Silver Links (*Toronto, Canada, 2004, and *Blue Cascades III (*Bellevue WA., 2006).
14. See Blue Cascades III: Managing Extreme Disasters, Final Report (released to public on April 27 and available through contacting PNWER at www. pnwer.org. The exercise, developed by the Puget Sound Partnership for Regional Infrastructure Security, was hosted by the Pacific NorthWest Economic Region (PNWER), a state-chartered consortium of five states (Washington, Oregon, Alaska, Idaho, and Montana) and three Canadian jurisdictions (British Columbia, Alberta, and The Yukon Territory).
15. Ibid., see Executive Summary.
16. Ibid.
17. Information is based on personal observations, a wide variety of lessons learned documents available on the Internet (search under "Hurricane Katrina Lessons Learns for Communications;" also see U.S. Government, The Federal Response to Hurricane Katrina: Lessons Learned, February 2006, 217 pp.
18. The *Guide* can be accessed and downloaded at www.tisp.org.
19. For the process to identify and bring together public and private organizations to begin to develop a regional partnership, see Ami Carpenter, Paula Scalingi, and Sandra Cheldelin, "Final Report, Vol. 12: Designing a Roadmap to Partnership: The First Step—Identifying the Key Stakeholders," Critical Infrastructure Protection in the National Capital Region, published by the University Consortium for Infrastructure Protection and managed by the Critical Infrastructure Protection Program of the George Mason University School of Law, September, 2005.
20. Patrick S. Roberts, "Reputation and Federal Emergency Preparedness Agencies," paper presented at the American Political Science Association Annual Meeting, Sept. 2-5, 2004, p. 9. Roberts notes that the 1950s through the 1970s was a period when the primary concern of disaster preparedness was a nuclear attack by the Soviet Union and the Defense Department dominated what was then called civil defense.
21. The day before Hurricane Katrina struck the New Orleans region, regional stakeholders were scheduled to meet for the last planning meeting for the Purple Crescent III interdependencies tabletop exercise. The scenario was a small nuclear device spirited into the city by domestic terrorists allied with U.S. adversaries overseas. One of the significant issues in developing the scenario was the impact on critical infrastructures of a blast, electro-magnetic pulse and radiation, as well as on buildings and other structures.

Measuring Resilience in Network-Based Infrastructures

David A. Garbin

Senior Fellow
Center for Information Technology and Telecommunications
Mitretek Systems
Falls Church, VA

John F. Shortle

Associate Professor
Systems Engineering and Operations Research
George Mason University
Fairfax, VA

Overview

A key component in the ability of the United States to survive the effects of catastrophic events, both natural and man-made, is the ability of our critical infrastructures to function following such events. A classical approach to this problem is to protect each of the components of the infrastructure against these effects. The commonly used term “critical infrastructure protection” derives from this approach. Shortcomings to this approach became apparent during the 1960s as the Department of Defense attempted to protect its domestic communications infrastructure from Soviet attack. The cost of protection is not linear with the intensity of the attack. A point is quickly reached where a small amount of extra protection incurs a large amount of extra cost. In the cat and mouse game of escalating attack capability and protection measures, a point was reached where individual components could not be protected from the threat (the telecom switches buried underground on sprung platforms could not survive the level of nuclear capability that could be delivered).

A new concept evolved whereby the loss of individual components of the infrastructure was taken as inevitable. Survival of the infrastructure then depended on reducing the effect of the loss of any individual component. Redundancy of key functions and the robust interconnection of components through networking improved the ability of the infrastructure to fulfill its mission under damage. This characteristic of network-based infrastructures was called survivability; today the term of art is resilience. It refers to the ability of infrastructures to degrade gracefully in the face of natural or man-made disasters. In the following sections, we will explore the benefits of quantifying network resilience as part of an overall risk assessment approach and will present a framework and methodology for deriving a resilience index for real infrastructures.

Network Resilience and Risk Assessment

Current infrastructure analyses utilize a risk management framework that combines threat, vulnerability, and consequence information to produce a comprehensive assessment of risk that drives risk reduction efforts. Typical risk assessment methodologies focus on the probability of a successful attack and a “consequence” factor for the infrastructure component. For network-based infrastructures, there is a non-trivial relationship between component failure and consequences of the failure. Networks have many alternate paths to carry commodities from place to place and, in theory, can be very robust with respect to component failures. Hence, any consequence factor related to a network must be formulated in terms of the network’s ability to fulfill its mission (i.e. carry its commodity from origins to destinations) under the damage scenario being applied. In order to assess this ability, there must be a common language to describe the attributes of networks and a mechanism for determining these attributes for real networks. Before delving into these details, let us examine the environment in which these networks exist and the current issues involved in increasing their resilience.

Why is Network Resilience Important?

Today, many key regional and national infrastructures are network-based. Examples include telecommunications, electric power, transportation, gas/oil, and water. Modern technology has made possible the sharing of resources over large distances through networks. The advantages of this approach include the ability to generate commodities in the most cost-effective places and deliver them wherever they are required. Networks can adapt to changing distribution patterns and efficiently handle peak demands by dynamically applying resources. Additionally, telecommunications networks provide the ability to monitor and remotely control a wide spectrum of other infrastructures. Although the many benefits of this paradigm are obvious, recent trends give some cause for concern.

Economic forces are driving an ever-increasing dependence on these regional and national networks. Applications such as just-in-time inventory management do not just improve efficiency; they become essential to the operation of the enterprise. Individual components, such as retail stores in a small area, cannot operate independently for any length of time if the network is compromised. These same economic forces, coupled with technological advancement, have created similar dependencies in the service provider sectors. Using telecommunications as an example, advances in fiber optic technologies now make it possible to carry almost infinite amounts of information over single strands of cable. Given the high cost of constructing facilities, carriers are deploying more and more traffic along fewer and fewer physical facilities. For regional and national networks, these long-haul facilities must be constructed along a restricted set of available rights-of-way (e.g. railroad beds, highways). As a result, even facilities from different carriers often travel along the same physical routes and will all fail simultaneously in the same damage event. Figure 1 illustrates this phenomenon for a typical national data network.

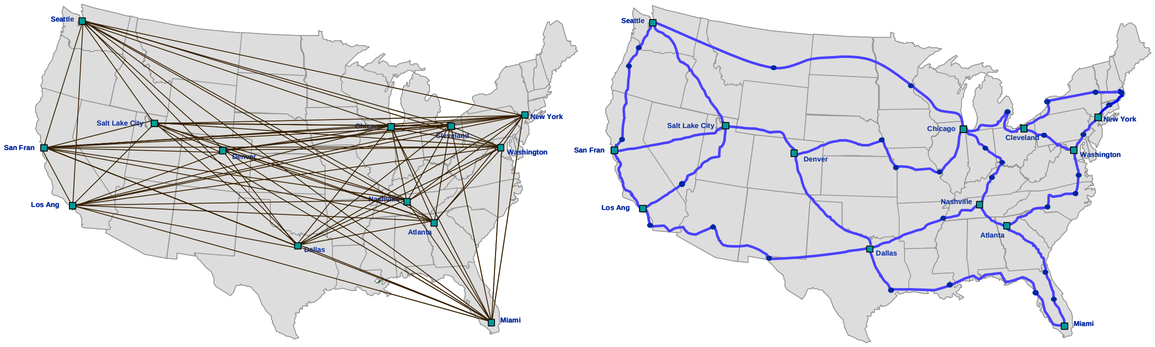

Fig. 1. Logical versus physical network connectivity

The left figure shows the logical connectivity among all the switches in the network. All switches are usually directly connected to all other switches over label switched paths, a logical entity created by routing tables in the network. However, these paths are carried over an underlying fiber optic network shown, on the right. This layout is typical of long haul fiber routes in the U.S. It can readily be seen that even a single fiber cut can have far reaching consequences. Careful establishment of backup paths with attention to the physical routing can provide protection against a single fiber cut, but most networks cannot handle multiple simultaneous failures. A real-world example of this phenomenon was the Baltimore tunnel fire of 2001 which melted fiber optic cables in the tunnel and disrupted all telephone and Internet communications along the East Coast and caused network congestion as far away as Los Angeles and Seattle. Similar widespread effects would result from damage to any one of a dozen "peering points" where all the major Internet carriers interconnect with one another.

Another type of hidden dependency is that of one sector's network infrastructure on another's. Some of these may seem obvious, such as telecommunications dependency on the electricity grid. But the dependence of the electricity grid on status information from its components reaching central control stations and the ability of these central stations to take corrective actions (i.e. the dependence of the electricity grid on telecommunications) is less obvious.

Vulnerabilities such as the ones mentioned above come about and are difficult to overcome because the critical infrastructures in the United States are largely created by private industry and not by the government. Investments to improve resiliency are often large and must be justified by a business case. This is difficult enough when the threat is of low probability, but it is impossible if the improvement in resiliency cannot be quantified. A measurable index of resiliency would go a long way toward quantifying the benefits of any investment.

Key Parameters for Describing a Network

The first step in network analysis is to define the set of parameters that, taken together, characterize a network in sufficient detail to make quantitative assessment possible. The details of these parameters may differ for different types of networks, but the concepts remain the same for all networks. Equally important is the ability to determine these parameters for real-world networks either through design documents or by direct, practical network measurements. The parameters fall into four general categories: demand, topology, capacity, and routing. For each category, the following sections discuss the parameters, the specific nuances of the parameters for different types of networks, and the issues with measurement of these parameters in real networks.

Demand

Demand, often referred to as "traffic" or "offered load" for most networks, is a measure of the amount of a commodity to be carried from sources to sinks by the network. The commodity is unique to the type of network (e.g. cars for transportation networks, power for electricity networks, packets for data communication networks). The level (intensity) of the demand can be characterized by a single unit of measure (e.g. megabits per second for data networks). However, there is usually a further breakdown which separates the size of a unit and the frequency with which the units arrive for service by the network (e.g. packets containing 2000 bits arrive every millisecond). Sources originate commodity traffic, and sinks consume that traffic. An important distinction is whether the commodity is fungible. Fungible commodities allow the flow from any source to be consumed at any sink. Non-fungible commodities have specific source-sink requirements which must be met explicitly. Electricity networks are an example of the former category, while communication networks fall into the latter (delivering traffic destined for Los Angeles to San Francisco is not useful).

Multi-commodity demand is often a difficult parameter to measure in large networks. Simple counters can measure the traffic on links in a network (e.g. the number of cars per hour using a roadway), but there is no easy way of knowing where the car originated or where its final destination is. In fungible commodity networks, it is sufficient to know source generation capabilities and sink consumption requirements, both of which are easily measured.

Closely associated with the level of demand are the performance requirements placed on satisfying the demand. Requirements are often expressed in terms of the following metrics:

1. Throughput – the amount of the offered commodity that is delivered to the destination
2. Loss – the percentage of the offered commodity that is not delivered to the destination
3. Delay – the amount of time it takes to deliver the commodity. Delay can be expressed either as an average delay or a percentile (e.g., 99.9% of the commodity delivered in less than 2 seconds).

The most basic requirement is throughput. For transportation and data communication networks, the time delay in delivering the commodity is also important. For many applications, the usefulness of the commodity at the destination is time sensitive; delivery outside of the required time frame is treated as a lost commodity.

A measure of consequence related to network damage must take into account the inability to meet all applicable performance requirements. In addition, different commodities may have different performance requirements related to these metrics. For example, in telecommunications, voice traffic must be delivered with low delay, while some packet loss is tolerated. Data traffic, on the other hand, requires low packet loss, but can tolerate some delay. Further, in response to network damage, network controllers may trade decreased performance in one metric for increased performance in another. For example, in aviation, airlines often cancel flights in poor weather (effectively making the “loss” metric worse) as a way to improve delay metrics.

Transmission link characteristics

Transmission links carry commodities between junction points, or nodes, in the network. A link may connect a source or sink node to a network node or it may connect two network nodes together. The former type is usually called an access link and latter a backbone link. Access links only carry traffic to and from user nodes while backbone links carry tandem traffic (also known as through traffic) on its way to the final destination. The essential characteristic of links is capacity (i.e. how much of the commodity can be carried by the link). The units of capacity are the same units used to specify the demand (e.g. megabits per second). The other related factor is how the commodity is admitted to the link and how the performance metrics are related to the level of demand and the link capacity. In the data communications example, packets wait in a queue to be served and the delay is related to demand level as a percentage of link capacity (see Figure 2).

For percentages equal to or greater than 100%, the delay grows without bound, and in steady-state, the delay is infinite. Practically, such unstable conditions are usually temporary and demand eventually falls below the link capacity. In such cases, a transient analysis of the network is required. For example, in aviation, when weather reduces airport capacity below the arrival rate, airplanes will be held at the departing airports until the weather improves at the destination airport. Effectively, this thins the schedule so that the period of over-saturation is temporary. For any type of network, the relationship between demand and capacity for links is generally known mathematically.

The end-to-end performance of a network is essentially a function of the performance of the individual links. Links are important because they are an especially vulnerable part of the network; a link in a national network may be several hundred miles long and can be disrupted at any point along its route. It is virtually impossible to protect a link along its entire length. Links are also vulnerable to natural phenomenon such as train wrecks, motor vehicle accidents, or being severed by digging equipment (a common occurrence).

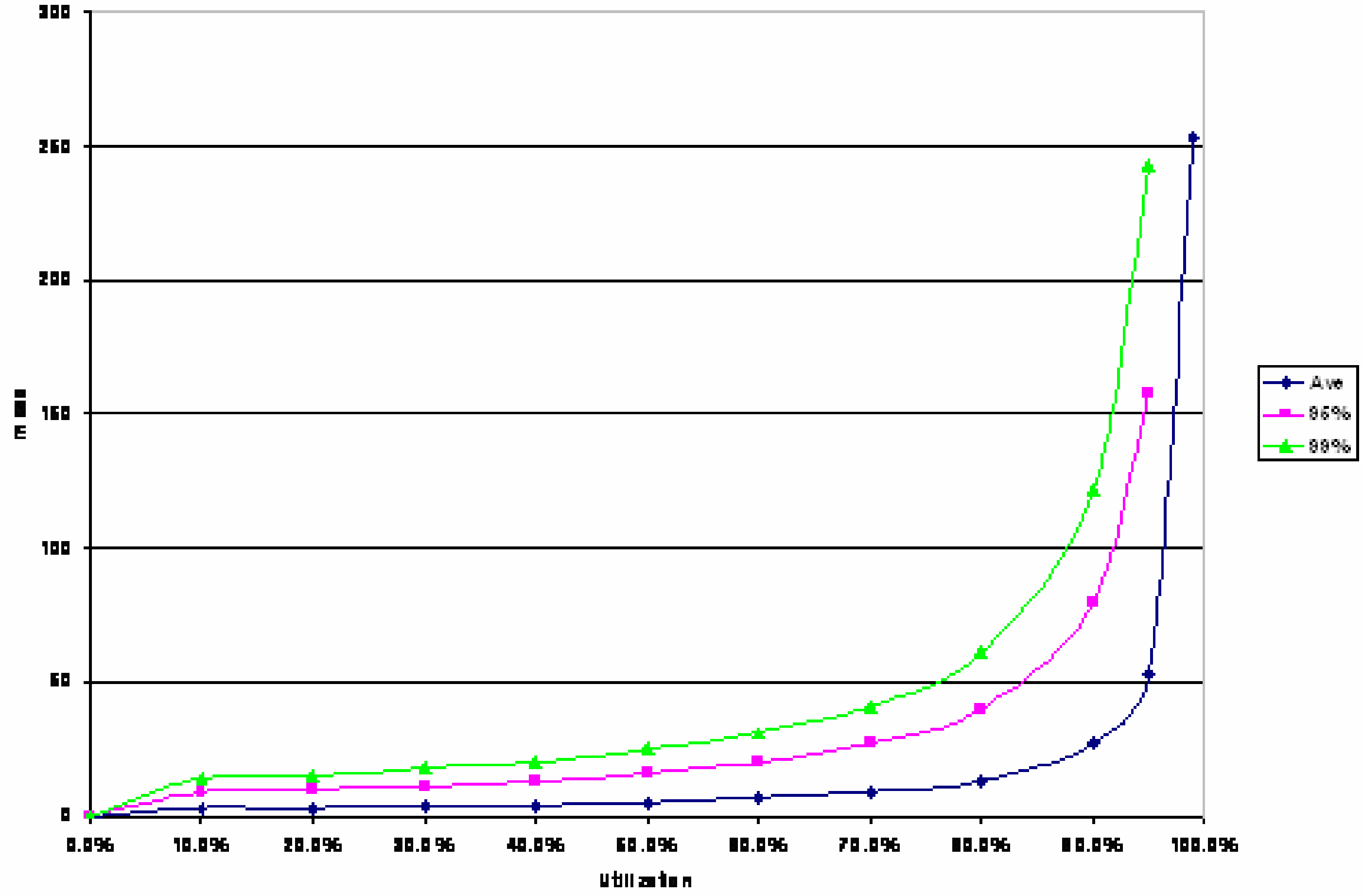

Fig. 2. Link delay (in msec) versus utilization (in %) in stable state

Junction node characteristics

As stated previously, junction nodes are connection points for the logical transmission links. The purpose of the junction nodes is to control the flow of the commodity from one link to another. Examples include interchanges on highways and switching nodes on communications networks. One characteristic of a node is its capacity. This can be expressed in terms of how many links it can terminate, what size links it can handle, and the total rate at which it processes commodity units. However, with respect to resiliency, the most important characteristic is how the node decides where to send the commodities passing through it and how these decision rules can react or be controlled during stress situations. In telecommunications, these rules are often referred to as routing rules and the mechanism for implementing them as routing tables. The routing characteristics of a network are dependant on the network type. For example, telecommunications networks employ physical routing tables that can either be predetermined and downloaded to the nodes or can be automatically generated by optimization algorithms in the nodes themselves. In electricity networks, once the connections are made between transmission links, the laws of physics determine the commodity flow. At the other extreme, routing in ground transportation networks is performed by the commodities themselves (those pesky drivers), while routing in air transportation networks is performed by controllers. During crisis periods, the existence of manual or automatic means to provide alternate routes for traffic and the ability to direct that traffic over these routes is a characteristic that must be captured and modeled in any resilience analysis.

The logical and physical topology of the network

The logical topology of the network refers to the connection of junction nodes by transmission links. Each transmission link connects two nodes, one at each end of the link. A commodity enters the link at an originating node and leaves at the terminating node. The link is called a logical one because the commodity may physically pass "unopened" through several intermediate nodes on its way to the destination. Routing tables use the logical topology to determine where to send a commodity next. The performance of a network is determined by the routing of commodities over these logical links and the relative demand offered to the link in relation to its capacity. *However, resilience of a network is more determined by the physical topology than the logical topology.*

As illustrated in Figure 1, logical links between nodes can be carried over an underlying physical structure. For example, many fiber optic cable strands can be carried in bundles buried along the same railroad tracks. In every city, strands can be broken out and connected to the node in that city, one from each city along the tracks east or west of that junction. Each strand represents a discrete logical link, but there can be only two physical links connected to the node. It is the physical links that suffer damage in any risk analysis, but it is the removal of the logical links that affect network performance. Hence, another important factor in network characterization emerges: the concept of shared risk groups.

Shared risk groups

In a network resilience model, shared risk groups are sets of links that fail together with the failure of a single physical facility. Since a given logical link can be carried over several physical facilities, it may belong to more than one shared risk group. As damage scenarios are modeled, each affected physical facility has all the logical entities in its associated shared risk group removed. Algorithms searching for network vulnerabilities look for groups or sets of groups that cause the most disruption of network traffic.

Formulating a Resilience Index for Networks

The first step in quantifying how a network reacts in a damaged situation is being able to characterize its performance under normal conditions. This involves knowing the network parameters as described above (in particular, the logical topology, the capacity of the logical links, and the routing tables) and formulating a demand profile to use as an evaluation case. This may be a normal busy period demand or it may represent the overload demand caused by the disaster event. This overload demand, as in the case of telephone traffic, may cause performance degradation in the network with no network damage whatsoever. As discussed earlier, typical performance parameters for networks are throughput, loss, and delay.

Simulations or analytic models based on queuing theory are used to predict the network performance under load. Under overload conditions, the throughput is an appropriate measure of network performance on which to base a resilience index.

Figure 3 shows an example of a resilience graph. Several resilience curves are shown in the figure. The horizontal axis represents the percentage of network components damaged in a given scenario. These components could be network links or network nodes or some combination. The vertical axis represents the network performance of a given scenario normalized by the network performance of the undamaged network (in a given overload condition). The point at (x = 0, y = 1) is the baseline scenario. Several examples of resilience curves are shown in Figure 4. The ideal (unachievable) case suffers no degradation in throughput until the entire network is damaged. A linear case has the same percentage reduction in throughput as the percentage of components lost. Real cases can fall on either side of the linear line.

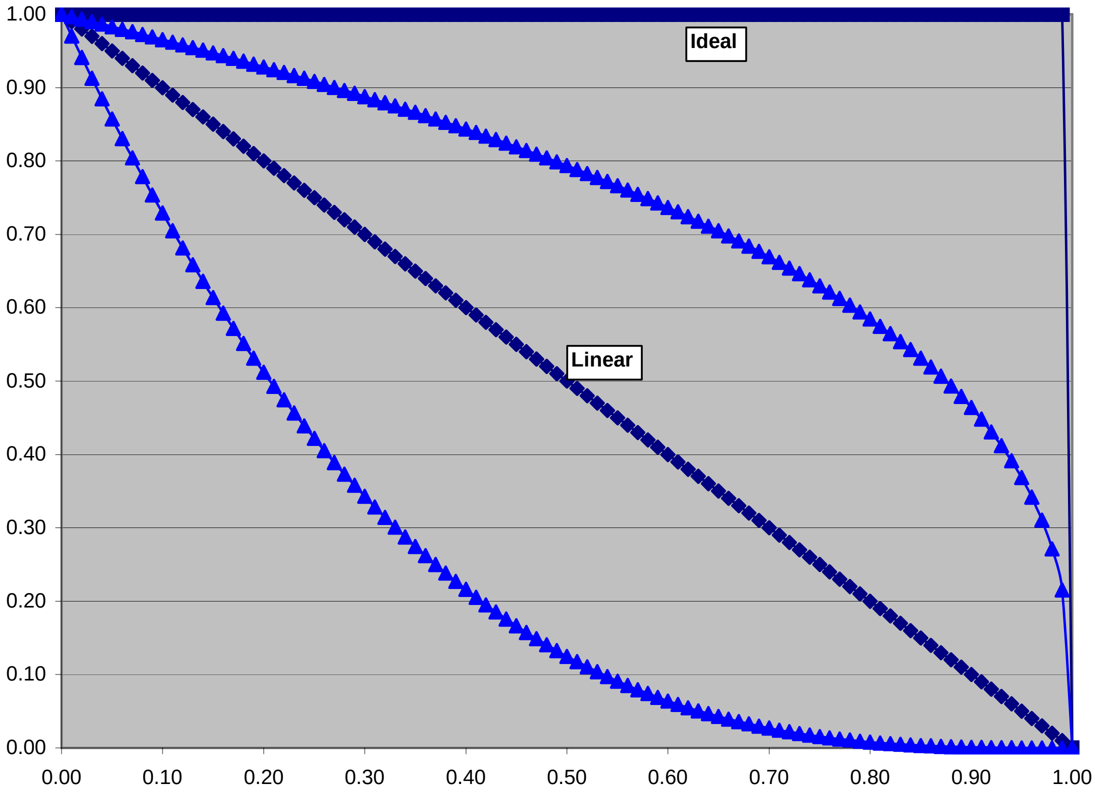

Fig. 3. Examples of network resilience curves

While the horizontal axis expresses the damage to network components as a percentage, the shape of the resilience curve is heavily dependent on the damage scenario chosen (i.e., which components to select for loss at each damage level). Several damage scenarios are possible:

1. Random damage
2. Optimum damage
3. Collateral damage from weather or non-directed attack

While it is useful to calculate the network performance degradation under specific scenarios for planning purposes, calculating a repeatable resilience index that can be used to compare network architectures requires a more structured approach. A measure that is comparable across different networks is how a network reacts to an optimum attack against its components. This is obviously a worst case scenario and the results would be expected to be worse than linear. Nevertheless, it is a good relative indicator of network resilience and will illustrate the benefits of proposed upgrades to improve resilience. Since network links are more vulnerable to damage than network nodes (because they are exposed to damage over a much larger area), a graph based on percentage of links damaged should be calculated as well as a graph based on percentage of nodes damaged.

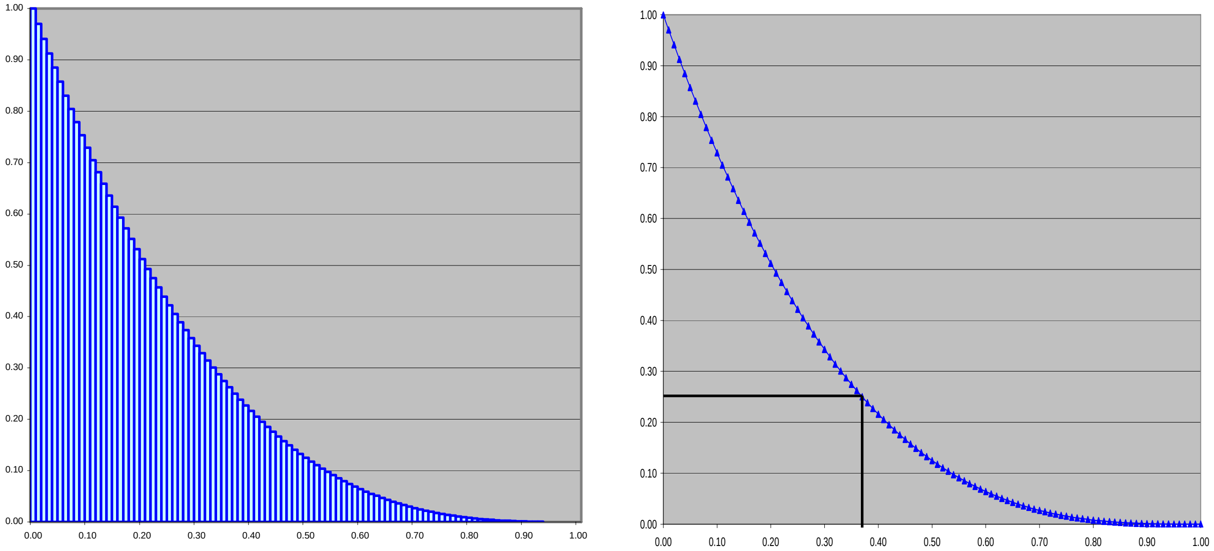

Fig. 4. Two possible definitions of a Resilience Index

The final step in the process is to assign a single number to represent the results of a resilience graph. Two possible indices to explore are shown in Figure 4. One index is the area under the resilience curve; the other is the percentage of commodity damage necessary to cause a threshold value of throughput reduction. How these indices behave under real network conditions is the subject of ongoing research at Mitretek Systems and George Mason University.

Methodology for Network Resilience Calculation

First and foremost, any methodology for determining a network resilience index must be implementable in practice. The initial challenge will be to determine the parameters which characterize the network under study. Some of these parameters can be readily determined from network design documents and as-built documentation. Others are more problematic and assumptions must be made in estimating these parameters. In some applications, the mapping of the problem domain to a network model may be non-trivial as well. For example, in aviation, the physical links representing possible flight paths are not cleanly defined, because aircraft are not restricted to fly along precise routes in the same way that cars are restricted to drive only on physically established roads. Once the input data are documented, a step-by-step process can be followed to derive the resilience index.

The logical network topology and component capacities of a network are the most easily gathered information. These are the result of a design process, and the components had to be built or procured. The specific values can be taken from documentation or, for some network types, can be queried centrally from the network components themselves. Where deterministic or algorithmic routing is used in the network, the routing tables or metrics used in well-known algorithms can be obtained from the network designers or the components. Routing parameters generally are more difficult to obtain than topology information as they are known to fewer personnel deeper in the engineering organization; nevertheless, the information is knowable and can be obtained.

The two most difficult categories of information to obtain are demand information and physical facility (shared risk group) information. In most networks, it is either impossible or prohibitively expensive to measure demand on an origin-to-destination basis. Each commodity would have to be inspected and its destination recorded to derive such information. There are measurements, however, that are routinely made in all networks: the utilization of individual components. Specifically, the average traffic carried on links over a specific time period is collected for engineering purposes. These statistics are gathered from simple counters or similar devices on each link or on the interfaces of the junction nodes where the links connect. If a set of consistent measurements is gathered from all links in a network, the demand matrix among the source and destination nodes can be estimated. The algorithm is aided if the routing in the network is known. While the solution obtained by this method may not be exact, it can provide a good basis for the resilience studies. Refining this process of deriving end-to-end demand from link measurements is a continuing research area.

Determining the shared risk groups for network links may be the most vexing and the most important part of the resilience index process. Within a single network type and facilities provider, there is a possibility of knowing how transmission links are carried over physical facilities. Even then, technology can sometimes make this difficult. In the telecommunications sector, the routing of logical links over physical facilities can be changed electronically and the state of this mapping at any given time is unknown to the end user. When many different providers are involved, there is no mechanism to capture sharing of rights-of-way across the providers. Most issues regarding shared risk groups occur in the vicinity of the end users and involve the “last mile” connections into the network nodes. The nature of these connections should be gathered from the end users themselves to determine if any special provisions have been made for diverse physical routing. For regional or national infrastructures, the physical rights-of-way available for facilities should be documented for the specific sector. This may involve proprietary information from the private sector companies involved, or may be available from government entities or industry associations. Effort put into this area at the outset of a project will pay large dividends in the fidelity of the results. On a national scale, documentation of utility rights-of-away across sectors would be a significant resource.

Given the demand, topology, and routing information, a baseline performance assessment can be made without damage to components. Damage scenarios can then be formulated against physical components of the network. The shared risk group information can transform these into logical network damage and a performance assessment can be made at that damage level. For each type of damage scenario (e.g., link only, node only), optimization algorithms can determine what specific component loss would cause the maximum performance degradation. Typically, "steepest descent" algorithms are used; best single facility outage is determined, then the next best, and so on. While this is not optimum, it is computationally efficient and provides a deterministic method of proceeding. If the network performance can be evaluated quickly enough, more sophisticated algorithms can be employed to find optimum multi-component vulnerabilities. Evaluating optimum attack algorithms against networks is another active research area within the resilience realm.

Improving Resilience of Network Infrastructures

One use of the resilience index is to provide a consequence factor in formal risk assessment studies involving critical network infrastructures. A parallel, and possibly more important, activity is the improvement of the resilience of networked infrastructures. This issue has two dimensions:

1. How do you know that the resilience of an infrastructure needs improvement?
2. How can you justify the cost of improving that resilience?

Both dimensions require a quantifiable measure of resilience as part of the answer. As mentioned previously, private sector investment in resilience requires a business case. The resilience index can provide the quantitative basis for the benefits portion of such a business case. In fact, optimization techniques can determine the most cost-effective network augmentations from a resilience standpoint.

Summary

Network-based entities are an increasingly important part of the critical infrastructure of the United States. Networks form the basis for fulfilling the missions of diverse sectors of the economy (e.g., telecommunications, transportation, energy.) In traditional risk assessment studies, the consequence factor related to network component damage is ill-defined. This paper has outlined an approach for measuring quantitatively the resilience index of a network. Research areas related to this measurement have been defined and the need to gather data on a national scale on critical network elements, such as utility rights-of-way, has been identified. The use of the resilience index in supporting business cases for network resilience improvement has also been noted.

Resilience: A Systems Design Imperative

David Arsenault

Research Associate
Department of Computer Science
George Mason University
Fairfax, VA

Arun Sood

Professor
Department of Computer Science
George Mason University
Fairfax, VA

Dangerous World, Dependencies, and Fragile Systems

There can be no doubt but that information systems and the networks that connect them have become mission critical to the operations of enterprises, functioning of economies, and defense of nations. Yet, these critical information processing systems remain vulnerable to faults, attacks, and their own inherent complexities, despite ongoing global attention to matters of security and availability following the September 11, 2001 attacks on the United States. In fact, The *President's Information Technology Advisory Committee (PITAC)* recently warned that "The IT infrastructure of the United States is highly vulnerable to terrorist and criminal attacks."[1] Other nations' infrastructure systems and those of global enterprises are likely to be equally, if not more, susceptible to the same phenomenon.

Despite decades of concentrated research on computer system and network security, availability, and fault tolerance, our systems remain fragile, brittle, and vulnerable. As modern societies, we depend increasingly on information systems to run financial markets, facilitate international trade, enable global telecommunications, manage transportation networks, and control utilities.

The computer hardware and software industries, national research labs, and academic institutions continue with valiant efforts to enable more robust, fault tolerant and secure systems. Some progress is being made indeed; many well-designed technologies exist to address specific systems challenges. However, these solutions tend to be reactive. Security problems become known, they are researched and often viable solutions are found. The resulting new tacit knowledge is then propagated forward into the next generation of hardware and software.

Even a casual survey of information systems literature will reveal a set of core concepts of system design such as availability, fault tolerance, recovery, survivability, reliability, continuity of operation, confidentiality, and integrity. Each of these, when examined more deeply, is a topic in and of itself. Further, many system designs require some combination of these concept. For example, computer security typically defines “security” as a triad of confidentiality, integrity, and availability—each with volumes of research, methodologies, and commercial products aimed at providing these benefits to information systems. Similarly, the fault-tolerant community deals with issues of reliability, recovery, and survivability, which are vital to systems where life or substantial economic resources are at stake—aircraft control systems, stock markets, banking, or telecommunications are prime examples.

Fault-tolerance and security, for the most part, are system level concepts. The techniques and technologies are applied in a bottom-up fashion starting with the individual data structures, functions, and modules within application programs. Individual application programs are combined either on the same physical machine or through a distributed system approach. Through this layering process we build complex systems and systems of systems. This same approach also builds systems that tend to be more brittle than expected with respect to faults or malevolent activities. While typical computer security and fault-tolerance implementations are machine-centric concepts, large scale and distributed of systems have design features to ensure continuity of operations, and this requires particular attention to the human dimension. In the face of large-scale destruction, it is not sufficient for the systems to survive, but, to maintain continuity of operations, a properly trained workforce is also essential. Resilience seeks to address these problems by taking a holistic top-down approach—a system of systems architectural approach.

A Systems Approach: Resilience

Why are our systems so brittle on a large scale? Why are they still susceptible to both internal and external faults despite active and diligent research? Why do many types of faults often cause unpredictable effects that cascade beyond the initial point of impact?

The answers to these questions lie in the intersection of three critical characteristics of large scale systems: connectivity, complexity, and interdependence. When these factors are balanced in both the macro scale and the micro scale, it is possible to achieve systems that exhibit what we will define as resilience.

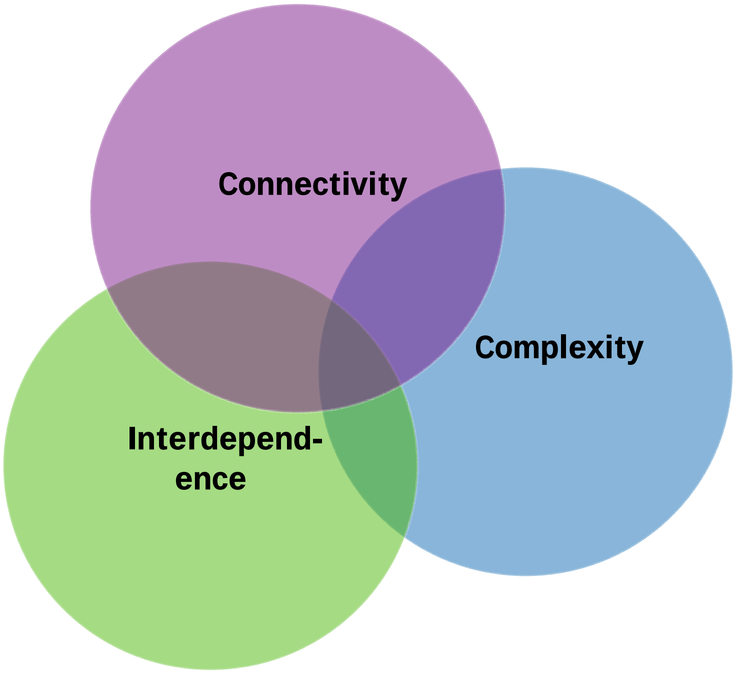

Fig. 1. Resilience is found in the intersection of connectivity, complexity, and interdependence.

Connectivity refers to fact that many individual systems are interconnected via networks to form larger systems of systems. The Internet, the air traffic control system, and power grids all demonstrate this principle. The most important systems used in today's society tend to be systems of systems. It is the interconnections between systems that add to their vulnerabilities. PITAC eloquently captured the importance of system interconnectivity with a simple equation:

Ubiquitous Interconnectivity = Widespread Vulnerability.[2]

Connectivity in complex distributed systems, if structured correctly, can also strenghten systems and provide additional assurances of robustness under adverse conditions.

Complexity invades our systems at all levels—in systems of systems (e.g. the entire banking "system" or even a single large bank), in individual systems (e.g. a foreign exchange trading platform), and in the components within individual systems (e.g. operating system, database, application server).

Interdependence stems from how complex our systems have become and the methods we use to deal with this complexity. To build complex systems of systems, we break the system down into services and link them together using networks. For complex individual systems, such as a transition server or database engine, we separate the functionality within the system into modules, and modules into classes and classes into functions and data structures. The common thread here is the interdependence of all of the parts within a system; only when the interdependent parts work correctly will the system produce the intended results, such as providing a set of services. Interdependence is both a positive and a negative.

A Multidiscipline View of Resilience

When we speak of resilience we focus on the functions that a system is designed to fulfill—clearing financial transactions, managing airspace, controlling power grids—not the individual components of the system or network. Physics and engineering disciplines define *resilience* as a physical property of materials: *the capacity of a material to absorb energy when it is deformed elastically, and then upon unloading, return this energy*. Ecologists have a more complex view of resilience in natural systems, and thus two completing definitions have emerged, each emphasizing a different aspect of resilience. One definition, known as engineering resilience, focuses on resistance to disturbance and the rate of return to equilibrium: *resilience is the rate at which a system returns to a single steady or cyclic state following a perturbation.*[3] The other view of resilience, specifically ecological resilience, focuses on state changes in complex systems: *resilience is measured by the magnitude of disturbance that can be absorbed before the system changes its structure by changing the variables and processes that control behavior within the system.* From a human perspective, resilience can be thought of as how well an organization can absorb unexpected challenges such as human error, malicious acts (insider threats), or the loss of key human assets.

These different domains each offer something of value when we consider what resilience means in terms of information systems. A multidiscipline, composite interpretation of resilience is most useful in our domain as it can and *should* inform us about how to architect systems that are better able to survive, and indeed thrive, in a dangerous world. Surviving means the system continues to provide the services it was designed to provide. Thriving means the system provides these services at acceptable levels of performance even in the presence of negative conditions.

Domain Models and Events

To further the concept of resilience as a multidiscipline holistic approach to systems architecture, it is useful to examine the models from well-developed domains, such as security and fault tolerance, as well as the types of events that drive these models. The following table provides a mapping between various systems domains and the characteristics we propose for resilient systems.

Table 1. Existing Domain Models Can Support the Resilient Systems Approach

Domain	Domain Models	Resilience Relationships
Fault Tolerance	Fault Models	Complexity, Interdependence
Availability	High Availability Models	Interdependence, Connectivity
Integrity	Integrity Models	Interdependence
Security	Vulnerability Models	Complexity, Connectivity
Resilience (ecological)	Perturbation Models	All Three Resilience Factors
Resilience (materials)	Shock Models	All Three Resilience Factors

Resilience in Nature

When seeking guidance on designing robust, large-scale systems that exhibit resiliency, we must seriously consider the critical lessons that nature has to teach us. There is a promising new science known as *biomimicry* which seeks to examine nature's models and then imitates or takes inspiration from these designs and processes to solve human problems, e.g., a solar cell inspired by a leaf.[4] Nature has much to tell us about how to build complex systems that work under forbidding conditions.

Interestingly, most systems in nature are systems of systems and are built from smaller components (i.e., cells and organs in mammals) that can exhibit surprising amounts of failure, yet the overall system maintains a minimum level of functionality—survival!

> The core idea [of biomimicry] is that nature, imaginative by necessity, has already solved many of the problems we are grappling with. Animals, plants, and microbes are the consummate engineers. They have found what works, what is appropriate, and most important, what *lasts* here on Earth. This is the real news of biomimicry: After 3.8 billion years of research and development, failures are fossils, and what surrounds us is the secret to survival.
>
> – Janine Benyus.[5]

Perturbation models from ecology and shock models from physical sciences can be applied to systems resilience most directly. Perturbation models provide the means to examine complex system behavior over time during periods of stress, as well as during periods of nominal operation. The key question here is how much can a system—in the macro sense, a system of systems—adapt to changes in operating conditions and still function nominally. By comparison, the shock model from materials science provides the framework for measuring and predicting the amount of energy a material can absorb as it is deformed (usually stretched, bent, or compressed) before it fails physically, which entails loss of one or more critical physical characteristics.

Central to most system perturbation models is the state of nominal operation of the system and abnormal operation (or failure) of the system with some triggering event or events that cause the system perturbation, which at some level of intensity creates a phase change in the system as it transitions from a state of nominal operation to that of the failure condition.

Table 2. System Perturbation Triggering Events

Event Type	Cause
Fault-driven	System fault (flaw or failure)
Availability-driven	Network outage, system outage
Security-driven	Exploited vulnerability (known or unknown prior to event)
Human-driven	Innocent error, malicious actions

Clearly other causes for these types of events exist, but the idea here is to classify and characterize the main types of events that can adversely impact a system. It is these types of events rather than specific details of a set of events that a resilient system must be architected to handle.

Resilience by Design

Functionality-Performance Tradeoff Curves

We define a *functionality-performance tradeoff curve* (FPT curve) to describe the behavior of a resilient system over a range of operating conditions as stresses or perturbation factors are applied. The Functionality-Performance Tradeoff Curve captures the relationship between functional richness and system performance. In terms of abstraction, two types of systems are considered when developing a FPT curve: performance-oriented systems and functionally-oriented systems.

Performance-oriented systems, as the name implies, place a premium on operational performance characteristics, such as end-to-end delay, transaction processing time, data throughput, or update speeds.

Functionality-oriented systems operate at the other end of the spectrum; for these systems timing is less important than maintaining a full spectrum of system functionality. The FPT curve for functionality-oriented systems will trade performance for richness of functionality when the system experiences stresses or perturbations.

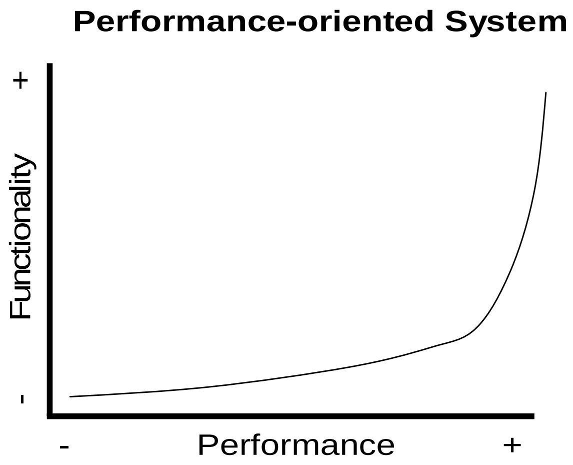

Fig. 2. Performance-oriented System

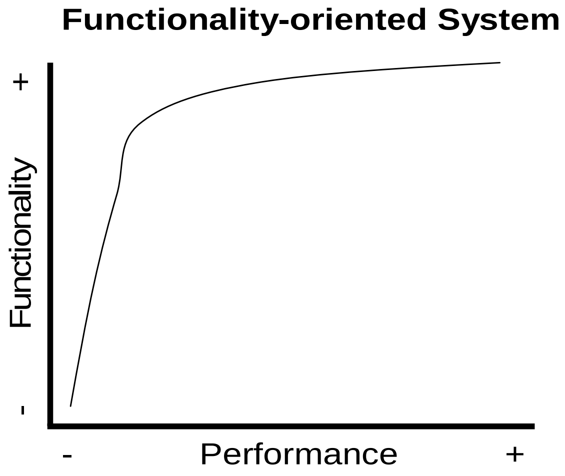

Fig. 3. Functionality-oriented System

Service Guarantees

Graceful degradation of services in resilient systems borrows from Service Level Agreements common in the application service provider domain. Formally defining how services can degrade to prevent an overall system failure is critical to maintaining system performance, functionality, or perhaps a blend of the two. Preventative actions such as shutting down certain services or throttling the performance of other services when systems experience stress can often make a significant difference in system stability.

Another, perhaps complementary, way to look at service guarantees is assured *minimum service performance.* Borrowing from quality of serive (QoS) concepts in data networks, the idea of assured minimum service performance involves issues of admission control (who can get into the system and when) scheduling (what actions to take when) and differential treatment of services (what requests are most important).

Prioritized Recovery

In an ideal world—which we know does not exist—systems would never encounter a situation where recovery is needed. In our formulation for systems resilience we need to provide for orderly and predictable recovery of services as systems attempt to return to nominal operating conditions following a significant perturbation.

Recalling the notion of prioritized recovery of services can be thought of as the micro-level recovery behavior of individual system services, servers, or applications which enmass produce the desired overall or macro system recovery behavior characterized using FPT Curves.

Resilience at Multiple Scales

To design resilience into our systems, we must look at the scale of such systems from two perspectives: top-down (macro-to-micro) and bottom-up (micro-to-macro). As such, we can view any complex system as a system of systems where each system (in the micro sense) is composed of several interdependent components. Some research challenges in the area of scale involve constructing resilient systems from essential unreliable individual systems, which are in turn comprised of unreliable components. Adding emergent and unpredicable behaviors of large complex distributed systems, including the human factor, make this a rich area for research.

Summary

This paper introduced the concept of resilience as the primary characteristic we must architect into our systems at all levels due to the risks and challenges posed by three convergent forces—connectivity, complexity, and interdependence. Taking a widely multidisciplinary approach to characterize what resilience can and should be, we have borrowed from network science, physical science, systems engineering, data networking, and social science.

Ongoing research is needed in resilience, specifically how complex systems are created and how they behave under stress. Much can be learned and leveraged from the growing body of knowledge in network science. Our future research will seek to advance the notion of resilient systems using network science as a basis for these efforts.

Notes

[1] Cyber Security: A Crisis of Prioritization. PITAC (February 2005) Available at www.nitrd.gov

[2] Ibid.

[3] For more on definitions of resilience, see http://en.wikipedia.org/wiki/Resilience

[4] For more on biomimicry see: www.biomimicry.net and *Biomimicry: Innovation Inspired by Nature.* Janine Benyus (HarperCollins. New York. 1997).

[5] www.biomimicry.net/faq.html

The Need for Resiliency at the Corporate Level

Darryl B. Moody

President and Chief Operating Officer
Resilient Corporation
Washington, DC

Introduction

For decades, the United States national policy and corporate operational emphasis has been on protection and security with respect to critical assets and infrastructures. This approach was useful in the old paradigm of defined threats and impending challenges such as Y2K and state-level enemy regimes. With the September 11 terrorist attacks, natural disasters, and other continued threats to our nation's capacity to maintain its citizens' ability to live their lives in a relatively secure manner, we require a new mindset and strategy. The nation must accept that 100% protection and security is unattainable, but maximizing *resiliency* is a must.

Resiliency applies at all levels: national, regional and corporate. At the national level, major infrastructure concerns and societal institutions must be robust enough, and unencumbered by legal and regulatory constraints, to serve the national good in normal operations, in crisis, and in recovery. At the regional levels, specific infrastructure assets come together in highly interdependent ways to serve local constituents and be a part of a national infrastructure. At the corporate level (which owns or operates the vast majority of our critical infrastructure assets), individual companies and operating units must ensure their business operations and service delivery capacities remain able to perform their primary business functions.

Resiliency, as described in this paper, should be adopted by all major companies. There can be clear business value to implementing a resiliency management process, from the upfront posture assessment through the on-going management of the organization, to maintain the desired level of resiliency. There are additional benefits for those organizations that own or operate critical infrastructure assets, as their level of resiliency impacts the resiliency of a geographic region, an industry segment, and ultimately, the nation.

Achieving resiliency in the U.S. requires both top-down and bottom-up approaches and actions across national, regional, and corporate levels. In the end, resiliency becomes the aggregation of business and investment decisions at the corporate level, occurring within regions, and hopefully contributing to national goals for resiliency. What is needed is an understanding of what critical infrastructure companies (and sectors) are willing to do and what unacceptable gaps remain that might harm regional or national resiliency. It is toward those gaps that effective programs and initiatives can be targeted by governmental agencies.

Put simply, we cannot have a resilient nation without first having resilient corporations.

This paper will provide an overview of the concept of resilience and apply it to the corporate level. The first part of the paper offers definitions and describes the evolution of various disciplines into the resiliency concept. Next, the paper discusses the application of resiliency at the corporate level and the motivation for its adoption. Finally, the paper discusses the potential roles of federal agencies in encouraging resiliency.

Resiliency Defined

The notion of resiliency is rapidly advancing as a practical response to the need to address a combination of security, preparedness, risk, and survivability issues in an effective way on multiple levels. Resiliency has no standard definition as of yet, but the various articulations share the same base meaning. Often the difference in the definition reflects the bias of the author, which might come from an information technology focus, or the business continuity planning world, or risk management. This author defines resiliency as "*An organization's capability to maintain its functions and structure in the face of internal or external change, and to respond positively when it can or to degrade gracefully when it must – consistent with its business interests and investment capacities.*"

To further clarify the definition, one can look to the conditions that speak to resiliency as within the following set of statements:

- Being resilient is a proactive and determined attitude to remain a thriving enterprise (country, region, or company) despite the anticipated and unanticipated challenges that will emerge.
- Resiliency moves beyond a defensive security and protection posture and applies the entity's inherent strength to withstand crisis and deflect attacks of any nature.

- Resiliency is the empowerment of being aware of your situation, your risks, vulnerabilities and current capabilities to deal with them, and being able to make informed tactical and strategic decisions.
- Resiliency is an objectively measurable competitive differentiator (i.e., more secure, increased stakeholder and shareholder value).

It is logical to expect that an organization that realizes the benefits of the above definition of resiliency will have a high likelihood of maintaining a successful and thriving enterprise.

Key Distinctions and Relationships

Resiliency is a comprehensive and overarching business concept that can serve to give context and unified purpose to many previously stove-piped initiatives across the enterprise. There will be some confusion for awhile in the resiliency discussion that is lexicon-based. This is understandable; because to date, resiliency has largely been addressed as an evolutionary outgrowth of various disciplines such as security, risk management, supply chain management, preparedness, crisis management, and business continuity. Professionals within those disciplines that have not fully accepted the broader nature of resiliency, often think of it as their discipline 'on steroids.' This does not do justice to the concept of resiliency. There needs to be an articulation of the distinctions and relationships between resiliency and some key component concepts to allow the broader concept to go forward.

The following discussions summarize the distinctions and relationships between the concepts and resiliency. In each case, they are considered a component of resiliency as defined in this paper, but significantly narrower in scope.

Resiliency and Security

Security, whether applied to physical, financial, personnel, cyber information, or any other asset, entails the measures to protect against danger or loss with emphasis on being protected from dangers that originate from outside. A significant breach in security could certainly impair an organization's ability to exist, and thus is a critical concept underlying the organization's capacity to be resilient. Resiliency is proactive in positioning a company to survive and thrive given known and unknown challenges. Security, as generally practiced, provides specific protection against identified or projected circumstances.

Resiliency and Protection

Protection is often associated with the set of actions to harden assets to withstand identified contingencies, mitigate the damage, or make them an unattractive target. The focus is to maintain the assets' core function and ward off harm. Typically, protection performance objectives are stated as an absolute capability against varying levels of threat (e.g. hurricanes, defined types of breaches, specific acts). Organizations plan for protection against specific threats or categories of threats. Resiliency approaches the issue from a standpoint of taking reasonable protective actions, but having alternative capabilities as needed, and the ability to withstand the disruption.

Resiliency and Crisis Management

Crisis management generally refers to the set of actions and capabilities in place to effectively respond to and contain a situation. The situation can vary from natural, man-made, or environmental challenges, whether internally- or externally-generated. Most consider crisis management to largely consist of actions that go into play when the crisis occurs and subside after it is considered "over". There are plans and preparations, but the actions are not often dealt with as part of normal operations. Resiliency depends on effective crisis management, but would encourage more prominent treatment of crisis management capabilities throughout the company's operation than is often the case.

Resiliency and Preparedness

Preparedness consists of the plans of actions for *when* the disaster or crisis strikes. Preparedness efforts are very specific sets of tactical actions (evacuation plans, sheltering plans, rehearsals, supply stockpiles, etc.) that the company and individuals will take to mitigate the effects of predicted disasters/crises. Resiliency requires prudent and serious attention to preparations for known likely disasters, particularly those that are highly likely (e.g., hurricanes in Florida). Resiliency would address preparedness as a specific emergency management business function, but more importantly, as being impacted by numerous functions across the organization. These may include human resources, strategic planning, financial management, information technology, and risk management.

Resiliency and Risk Management

Risk management consists of formal processes to identify threats and vulnerabilities to the company, and the mitigation approaches it will employ. Risk management is highly sophisticated and the results have application in managing the business, insurance coverage, and in attracting investors. The risk management profession is moving toward a more proactive and return on investment focus, but the traditional focus has been defensive in nature. Identifying and managing risks, particularly operational risks, is arguably the most important factor in achieving resiliency; however, it is one of many factors. Resiliency has a healthy consideration of posturing for future opportunities. That is not a traditional consideration in risk management.

Resiliency and Business Continuity/Disaster Recovery (BC/DR)

BC/DR has traditionally been advanced and is most mature in the context of information technology capacities. BC/DR considerations have increased in importance as the information technology assets they were originally designed to protect have become inextricably intertwined with critical business processes across the enterprise. Couple this with a decreased acceptance of downtime in critical business functions, and we find BC and DR planning now a priority for the C-Suite and Boards of Directors. BC/DR is also an important aspect of being resilient, particularly if the company addresses the full range of actions outside of the IT arena necessary to achieve continuous operations of critical business functions.

Additional areas could be included on the above list, such as emergency management, mitigation, and recovery. Each will also be narrower in focus than resiliency. They are also most often subjects dealt with by governmental agencies, versus companies—the focus of this paper. Dealing with the lexicon issues surrounding resiliency and rationalizing how the various disciplines, such as the above, are brought together to form a comprehensive view of resiliency will take some time, leadership, and effort over the next one to two years.

Evolution of Resiliency

The concept of resiliency is not new, and a number of leading organizations have engaged in addressing it from various perspectives. The number of entities has increased over the past two years, as has the volume of research and discussion. Some of the members of the resilience community are described below.

- Resiliency has been prevalent on the international front with national-level programs and initiatives advancing the concept in various countries such as the United Kingdom, Singapore, Israel, and Australia. These programs have targeted enhancing the survivability and continuity of major infrastructure systems, that are often publicly controlled, as well as the resiliency of populations.
- A few large U.S. companies, including IBM and Booz Allen Hamilton, have advanced resiliency. The products and services offered by these companies have been information technology-focused and address business continuity capabilities as the foundation of being resilient, although some have addressed the needed organization and human capacities to change and be agile.
- A number of boutique consultancies specializing in crisis management and business continuity planning have defined resiliency as the next step in the evolution of their domain specialties.
- A number of prominent academic institutions have established programs and centers to address resilience such as the Ohio State University and its Center for Resilience and the Massachusetts Institute of Technology (MIT). Again, the institution's approach to resiliency typically leverages their most prominent functional or domain expertise. That orientation might be supply chain management, engineering systems, or a legal aspect.
- Think tanks such as the Council on Competitiveness, The Conference Board, and the Council on Foreign Relations have engaged in resiliency discussions. Their perspectives have ranged from resiliency as a corporate strategy issue to resiliency as a national security issue.
- Most encouragingly, Industry-led associations have taken up resiliency, to include the Financial Services Sector Coordinating Council[1] and The Infrastructure Security Partnership (TISP). Those perspectives have addressed resiliency as an evolving, industry-specific approach to integrated risk management, as well as geographic regional resiliency of critical infrastructures.

The good news is that no approach to resiliency has been "wrong" or misguided. As the concept matures into something more comprehensive and pragmatic for U.S. businesses and organizations, it will certainly leverage the groundwork laid to date. Resiliency's most prominent manifestation has been in the information technology areas. That is now changed—and none too soon. Resiliency is now a C-Suite matter.

The Essence of Being Resilient

Resiliency is emerging as a proactive and empowering paradigm to strategically manage an organization to achieve competitive advantage and sustainability in a climate of dynamic threats, regulatory impositions, and fierce competition. A resilient organization deflects deliberate attacks and natural disasters (or their effects), absorbs unavoidable damage, and resumes operations to pre-event levels—*quickly*. This same capacity allows organizations to maximize their abilities to identify and pursue new opportunities, and operate effectively in normal times. In today's world, the events that impact an organization's resiliency are asymmetrical, constantly evolving, and rapidly impacted by technology improvements. Thus, resiliency must be an underlying management construct within a business operation—especially one associated with a critical infrastructure asset.

Resiliency encompasses strategic, risk management, operational and crisis management, and security elements. Resiliency forces a cross-functional view of functions, the existence or opportunities for synergies, and deficiencies that impact resiliency, which is not attainable by focusing on these elements in a stand-alone manner.

Progressive organizations have adopted risk management protocols, advanced security methods, and disaster and crisis management regimes. But with all that planning and implemented methods, exactly where does the organization stand in being resilient? Has it efficiently allocated resources and attention to the factors that impact resiliency? From the standpoint of being able to withstand a crisis situation or a significant opportunity, what is the level of situational awareness afforded to executive leadership?

Driving the organization to being resilient provides the on-going management focus that better ensures the organization is proactive and empowered to answer the above questions and to face its challenges and opportunities.

Resiliency Requirements

One could amass a daunting inventory of pressing requirements on today's CEO and Board Member of large publicly traded companies. The litany of laws, regulations, and expectations are overwhelming as individual dragons must be slain one at a time. But they should be addressed under a rubric of resiliency because many of the aspects of the requirements have converged across previous stove-piped operations and support domains within the company. For example:

- Preparedness for continued operations in a pandemic situation requires secured virtual computing capabilities.
- Accurate reporting under Sarbanes-Oxley requires systems with adequate controls operating reliably.
- Sarbanes-Oxley requires disclosure of significant business risks and vulnerabilities to investors.
- Recovering from a disaster/crisis situation may require adequate staff tracking capabilities with the HR systems that are then linked to secure systems for recall and communications.

Compliance, and the lack thereof, now presents a significant and real danger and risk in corporate America. Tremendous corporate resources are expended in reporting to regulatory agencies and the SEC—far more than in response to homeland security requirements. With the Sarbanes-Oxley requirements, the consequences of compliance failures have become severe and personally risky to executives. Thus, in addition to potential disruption from terrorist events, natural disasters, hostile takeovers, and market factors, companies could see missteps on the compliance front become a crippling and devastating event. The compliance requirements are coming from many angles: privacy, security, corporate governance, environmental, labor, trade and financial reporting. Protection against this onslaught is impossible, but companies must learn to be resilient against the effects and impacts.

Resiliency requirements will be specific to the company for some time before standards merge or any mandates are levied by governmental or regulatory agencies. There are standards that relate to components of resiliency, such as the NFPA 1600 standard for disaster/emergency management and business continuity programs. Information technology security management is governed by international standards, and numerous industry-specific standards are in existence. None of the existing standards are broad enough in scope to address resiliency, and it is doubtful that any will emerge in the near future. Until then, industry best practices will likely be the backbone of resiliency requirements.

Achieving Resiliency

Every organization is at some level of resiliency right now, but the question is whether it is the desired level. Being at a low level may be a business decision made because the organization is not willing or able to invest in the ability to bounce back from a disaster or crisis. Or, it might say that the expected level of performance in key areas that impact resiliency is not being achieved. Being highly resilient is a business decision to ensure that those functions, capabilities and operations necessary to bounce back are indeed in place and being performed acceptably. However, maximizing all capacities that are required for resiliency is simply not affordable and with the ever-changing environment, not likely to be achieved.

There cannot be uniform measures or expectations of resiliency. Why? Because levels of resiliency are a direct result of investment and business decisions made by organizations that are consistent with their individual constraints and interests. Companies are free to adopt a strategy of operating their business during "fair weather" and carrying enough insurance to cash out should a negative event occur. They can also be determined to withstand and recover from the most severe of blows and build the capabilities to give them the best chance to do so. These represent two different and legitimate business operational strategies with different levels of absolute resiliency. But both strategies meet the companies' resiliency objectives. By analogy, a small sailboat is not as resilient in a heavy storm as is a battleship, but if the intent and need is to sail on the lake on sunny days, the sailboat meets resiliency expectations.

Achieving resiliency can follow a typical management action cycle of logical steps. The first step is to understand where the organization stands in performing those actions necessary to be resilient. Creating this situational awareness of current resiliency posture should not be a costly or lengthy effort. The organization should then articulate objectives for its level of resiliency. This must be done by senior leadership. Considering the resiliency posture and the organization's resiliency objectives, management can then decide where to place attention for adjustments/enhancements to best meet business resiliency objectives. Next, companies would plan and execute specific projects to enhance their overall resiliency posture. This would likely mean reallocating capital to initiatives that provide a greater resiliency 'bang for the buck.' Progressive companies would implement management processes and systems to monitor their resiliency posture given changes in threats, their vulnerabilities, new technologies, or opportunities. Resiliency management becomes an on-going process.

Motivating Adoption of Resilience

Resiliency, as described in this paper, should be adopted by all major companies. There can be clear business value to implementing a resiliency management process, from the upfront posture assessment through the on-going management of the organization, to maintain the desired level of resiliency. There are additional benefits for those organizations that own or operate critical infrastructure assets, as their level of resiliency impacts the resiliency of a geographic region, an industry segment, and ultimately, the nation. However, since there are no governmental or regulatory mandates, some wonder what would motivate industry leaders to put an additional requirement on their plate voluntarily. The following present some compelling motivational factors.

1. Resiliency and the management of resiliency makes good business sense for a company, providing an empowering paradigm to have the situational awareness of a company's capacity to withstand crisis and to make informed decisions on what to fix.
2. The company's resiliency posture could be relevant and valuable information for the insurance industry in understanding the risks and inherent mitigation capacity, and thus could provide a market incentive to the company.
3. The company's resiliency posture could be relevant and valuable information to the investment community, to include rating agencies and financiers, affecting the company's ability to acquire capital and the costs, thereby providing a market incentive to the company.
4. The company's resiliency posture could be considered relevant to the health and viability of a public traded company, therefore a reportable condition in SEC filings and motivating the company to address deficiencies on an on-going basis.
5. The collective resiliency posture for an industry could be useful in informing or pre-empting regulatory and legislative actions, thus inviting encouragement of adoption from the industry associations.
6. For critical infrastructure owners/operators, the importance of their company's resiliency level to infrastructure resiliency at all levels is sobering and worthy of addressing with the many companies that are leading corporate citizens.

The current moment in time provides the opportunity for industry to step up to this new paradigm in their interests. Doing so pays benefits to industry while supporting a national goal of enhanced resilience. Doing so also positions industry to be proactive in working with legislators and regulators to work towards a mutual goal of resiliency.

Federal Government Role

Although resiliency is a corporate C-Suite issue, there is a necessary and valuable federal government role in advancing and supporting the concept and its effective implementation. The federal government should adopt the positive and proactive definition and attitude of resiliency offered above. Governmental entities on the legislative, administrative, and regulatory sides should support it through encouragement (and potential incentives) to public and private sector organizations. There should be a call for entities to achieve levels of individual resiliency which will lead to aggregate levels of resiliency that cascade up to national levels of resiliency. The critical difference in this approach, however, is that the individual levels of resiliency begin by being aligned with the organizational business or operational interests. The simple reality is that achieving regional or national levels of resilience is completely dependent upon leadership at companies making business and investment decisions that first meet their shareholder interests. An approach is needed to align those business interests with resiliency enhancements, maximizing the possibility that the private sector will make such investments.

It is unclear where the federal government leadership should come from. There are a number of possibilities: the Department of Homeland Security, the Department of Commerce, the Securities and Exchange Commission, the Office of Management and Budget, or the Congress. Each of these entities could play an effective facilitative role, but must avoid attempts to exert undue influence and control over industry, which must make the necessary investment and business decisions to achieve resiliency. This has been a great cause of concern and frustration on the part of industry and cited as a barrier causing the lack of progress in enhancing security and protective measures.

The ***Department of Homeland Security*** (DHS) has clear responsibilities for facilitating the enhanced protection of critical infrastructure assets and in the preparedness for emergency situations, natural or man-made. In January 2006, the Homeland Security Advisory Council (HSAC) recommended to the DHS Secretary that resiliency be adopted as the top-level national goal for dealing with the nation's critical infrastructure.[2] The HSAC concluded that the goal of protection should be replaced by a more realistic and measurable set of cascading national goals of resiliency. The HSAC also wrote that if resiliency was described in terms that corporate America could understand and that are consistent with their market charters, real progress could be made in motivating those that own and operate 85% of the infrastructure to enhance the protective posture, and through the collective efforts, enhance overall American security.

The ***Department of Commerce*** mission is to create the conditions for economic growth and opportunity by promoting innovation, entrepreneurship, competitiveness, and stewardship. The Department previously managed critical infrastructure protection programs now under the auspices of the DHS. However, various aspects of the Department have mission activities that can promote the adoption of resiliency concepts within the business community. For example, the National Institute for Standards and Technology (NIST) would be involved with consideration and development of performance standards for resiliency. With a long history of effective partnership with and advocacy for the business community, Commerce is positioned to have an effective leadership role in encouraging resiliency.

The ***Securities and Exchange Commission*** (SEC) mission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. The resiliency definition offered in this paper makes it a shareholder value concern, and thus the SEC's regulatory purview over companies whose securities are publicly traded comes into play. The levels of corporate resiliency can be considered a material matter, the knowledge of which could reasonably affect an investor's decision-making and therefore, a disclosure and reportable requirement on companies. This indirect influence and encouragement of resiliency could be extremely powerful, as businesses will undoubtedly pay more and on-going attention to that which is reportable in SEC filings.

The ***Office of Management and Budget*** (OMB) is positioned to have an indirect influential role in advancing resiliency as a national level goal. Through guidance issued via memoranda or circulars, OMB has significant impacts on how private sector companies (particularly those servicing the government) address numerous issues like privacy, information security, and personal identity management. OMB encouragement of resiliency of the private sector suppliers to federal agencies, along with the reporting of levels of resiliency attained, could advance resiliency adoption.

The ***Congress*** has a role in validating resiliency as a national policy goal and providing the platforms to advance resiliency. Through funding of administration programs to address resiliency and the conduct of hearings to assess the nation's resiliency status (by industry sector or by geographic areas), the Congress can provide an effective spotlight and bully pulpit to increase actions to enhance resiliency.

The Federal Government can provide an impetus for action with respect to adopting resiliency. Various federal agencies currently have missions that touch on resiliency and they are starting to lean in that direction, evident in the HSAC recommendation. Additional federal level entities could play a role in advancing resiliency. However, the overarching consideration must remain that resiliency investment is a business matter at the corporate level and federal imposition must be judicious. The true power of the movement to resiliency can lie in its voluntary adoption by industry, thus federal government intervention ought to be the minimum necessary.

Summary

The time for a focus on resiliency is here. Much groundwork has been laid across the various business management and technical disciplines that are required to achieve resiliency. As each of those disciplines has evolved, a common concept of resiliency has emerged. Clear benefits can be articulated to the stakeholders with respect to a company's level of resiliency. There is work to do in rationalizing the lexicon of resiliency and its components, but the level of consistency is more than enough to proceed with implementing the concept across industry—particularly the community of companies that own or operate the critical infrastructures of the United States.

Notes

[1] Homeland Security Strategy for Critical Infrastructure Protection in the Financial Services Sector, Version 2, May 2004

[2] Homeland Security Advisory Council, Report of the Critical Infrastructure Task Force, January 2006

Appendix

Resilience Background in National Policy

Elizabeth M. Jackson

Senior Associate, Special Projects
Critical Infrastructure Protection Program
George Mason University
Arlington, VA

The following information on select resilience studies expounds on the concept of resilience and demonstrates the need for additional considerations of this important concept.

National Infrastructure Advisory Council

The National Infrastructure Advisory Council (NIAC) discussed resilience in recent years, proposing specific topics for study and recommending related actions to the President and Secretary of Homeland Security. In April 2003, the Council proposed a study to address guidance on best practices for industry, stemming from regulatory guidance found in the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*.[1] Another proposed topic of study was the identification of non-redundant services within the Telecommunications Sector as they relate to the Banking and Finance Sector;[2] this topic was soon explored by the Financial Services Task Force. The dependence of these two millisecond sectors is obvious, as is its affect on the economy. Without diverse and redundant systems and networks, resilience is severely hampered.

The NIAC's Financial Services Task Force studied the Banking and Finance Sector's resilience concerns, specifically physical elements affecting resilience, and the Sector's vital dependence on the Telecommunications Sector. In its report to the President, the Task Force stated the following:

- Comprehensive business continuity planning and practices are essential,
- National security and emergency preparedness functions should acquire the highest levels of telecommunications resiliency assurances available. The continuity of the payment, clearing,

and settlement processes of the financial services sectors is critical to the overall economic security of the nation, and

- Public policy options are needed to stimulate investments. From a public policy perspective, appropriate mechanisms to stimulate market investments would enhance the National Security Emergency Preparedness (NSEP) telecommunications resiliency and should be identified.[3]

In its July 2003 Interim Progress Report, the Working Group on Cross Sector Interdependencies and Risk Assessment Guidance asserted that there should be incentives for private sector companies to spend funds on strengthening resilience.[4] The group restated this assertion in October 2003, noting that “organizations have been forced to take a proactive stance on securing their own resiliency” to protect themselves.[5] This action spurred change in numerous sectors as companies became more aware of the need to develop greater resilience to secure their operations from potential attack. Additionally, the notion of establishing a working group to focus on the need for resilience incentives was presented at the January 13, 2004 NIAC meeting.[6]

The importance of resilience was also voiced at NIAC meetings by Secretary of Homeland Security Michael Chertoff following Hurricanes Katrina and Rita. In October 2005, he stated that “[p]art of what protects infrastructure is the ability to work around damage and to bounce back after it has been inflicted.” [7] He recognized the cascading effects of failure in a critical sector and acknowledged that resilience can mitigate those negative effects in disastrous situations. Engagement of sector stakeholders at all levels, whether the local owner/operator or the Federal government, was deemed crucial to preparedness efforts in that “any business with a continuity plan, redundancy, resiliency, or the ability to continue work around damage was better prepared than those without it.”[8]

Most recently, in considering resilience in the private sector, the NIAC’s Intelligence Coordination Working Group (ICWG) acknowledged the inherent need to balance protection and resilience. In its final report on public-private sector intelligence coordination, the group stated that:

> CEOs recognize industry needs an understanding with the government about striking a reasonable balance between preventive hardening, on the one hand, and recovery and resilience, on the other. . . . Companies have built resilience for many kinds of threats into their business practices. Resilience is a lot less expensive than trying to protect against all threats.[9]

Continuing NIAC work focuses on improving homeland security, whether it is through enhanced protection, resilience, or overall understanding and awareness of risk.

Homeland Security Advisory Council

The Homeland Security Advisory Council (HSAC) Critical Infrastructure Task Force (CITF) is "charged with reviewing the current state of critical infrastructure protection policy and providing recommendations to further its objectives."[10] With this review, it focused on recommendations to shift policy from critical infrastructure protection (CIP) to critical infrastructure resilience (CIR).

Dr. Ruth David, CITF chair, stated that resilience-based strategies address the "full spectrum of threats, risks and consequence – including insider and criminal threats, accidents, natural disasters and terrorist attacks." [11] In doing so, resilience adds to protection efforts, complementing measures already in place and enhancing those areas of greatest significance to overall operations. Resilience also takes into strong consideration interdependencies, single-point vulnerabilities, and critical nodes of failure.

The CITF issued a report detailing its findings in January 2006. In its transmission of the CITF report to the Secretary of Homeland Security, the HSAC outlined recommendations that included "promulgat[ing] Critical Infrastructure Resilience (CIR) as the top-level strategic objective – the desired outcome – to drive national policy and planning." [12] Other key recommendations regarding resilience included the creation of "cascading national goals" and "an information sharing regime explicitly linked to critical infrastructure resiliency goals and governance."[13] The report elaborated on these recommendations, stating that CIR supports risk management and will align the efforts of government and the private sector in a more effective manner than with CIP alone.

Of note, the CITF's report acknowledged that resilient infrastructures:

> [A]re essential to continuity of business operations; to the successful execution of emergency response operations; to the maintenance of social stability; to the functioning of our economy; and to the advancement of our Nation's freedoms and quality of life.[14]

Moreover, the CITF asserted that resilience-based strategies *integrate* the three components of risk (threat, vulnerability, and consequence), demonstrating a holistic view of security our Nation's infrastructure. Resilience allows for the prevention of attack through reduced threat, defense from, or during, attacks through reduced vulnerabilities, and systems recovery from an attack through reduced consequence.

Like NIAC studies, CITF research found that business continuity plans and resilience go hand-in-hand. The CITF encourages use of business cases to justify resource allocation and funding for resilience, and has noted that solid business cases may avert unwelcome regulation of industry. With most business plans addressing infrastructure security or CIP and disaster recovery, resilience complements overall risk management and is becoming a greater focus of such plans. Business continuity plans also tie directly to the robustness of a system, network, or asset. Government consideration of these plans is essential to further development of the public-private partnership, a partnership focused on enhancing the security of our Nation's infrastructure.

As of the CITF report's completion, the U.S. Department of Homeland Security's (DHS) revised draft National Infrastructure Protection Plan (NIPP), while more focused on protection, also recognized the intrinsic need for resilience. Despite this, the CITF, and the HSAC by extension, recommended DHS incorporate more of "broader resilience objective" into the NIPP.[15] In response, DHS remarked that resilience is being woven into the Department's strategic plan and that it will be taken into consideration in preparedness, response, and recovery planning.[16] Notably, the CITF also called for a modification of Homeland Security Presidential Directive (HSPD)-7 to ensure consistency among policy documents.

Notes

[1] This paper was published by the Federal Reserve Board, the Department of the Treasury's Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission (SEC) on April 7, 2003. See Securities Exchange Act Release No. 47638 (April 7, 2003), 68 FR 17809 (April 11, 2003).

[2] Eric T. Werner, "National Infrastructure Advisory Council Minutes: Memorandum to Members re: Possible Topics for Study," 5. (April 17, 2003). Available online at: http://www.dhs.gov/xlibrary/assets/niac/NIAC_Minutes_042203_Final.pdf.

[3] National Infrastructure Advisory Council, "Meeting Minutes and Briefing Materials for April 13, 2004 Meeting," 26. (April 13, 2004). Available online at: http://www.dhs.gov/xlibrary/assets/niac/NIAC_Final_Minutes_041304.pdf.

[4] Martin G. McGuinn and Susan Vismor, "NIAC Working Group on Cross Sector Interdependencies & Risk Assessment Guidance Interim Progress Report," (report presented to the National Infrastructure Advisory Council, Washington, DC, July 22, 2003). Available online at: http://www.dhs.gov/xlibrary/assets/niac/NIAC_Minutes_072203.pdf.

[5] National Infrastructure Advisory Council, "Meeting Minutes and Briefing Materials for October 14, 2003 Meeting," 26. (October 14, 2003). Available online at: http://www.dhs.gov/xlibrary/assets/niac/NIAC_Final_Minutes_101403.pdf.

[6] National Infrastructure Advisory Council, "Meeting Minutes and Briefing Materials for January 13, 2004 Meeting." (January 13, 2004). Available online at: http://www.dhs.gov/xlibrary/assets/niac/NIAC_Final_Minutes_011304.pdf.

[7] National Infrastructure Advisory Council, "Meeting Minutes for October 11, 2005 Meeting," 5. (October 11, 2005). Available online at: http://www.dhs.gov/xlibrary/assets/niac/NIAC__MtgMinutes_10-11-05.pdf.

[8] Ibid.

[9] National Infrastructure Advisory Council, "Public-Private Sector Intelligence Coordination: Final Report and Recommendations by the Council," 30 & 32. (July 11, 2006). Available online at: http://www.dhs.gov/xlibrary/assets/niac/niac_icwgreport_july06.pdf.

[10] Homeland Security Advisory Council, "Summary of Meeting Held on June 23, 2005," 3. (June 23, 2005). Available online at: http://www.dhs.gov/xlibrary/assets/HSAC_MtgMinutes_June23-05.pdf.

[11] Ibid, 4.

[12] Homeland Security Advisory Council, "Transmittal Letter for Report of the Critical Infrastructure Task Force." (February 14, 2006). Available online at: http://www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf.

[13] Ibid.

[14] Homeland Security Advisory Council, "Report of the Critical Infrastructure Task Force," 1. (January 2006). Available online at: http://www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf.

[15] Ibid, 6.

[16] Homeland Security Advisory Council, "Summary of Meeting – Public Session," 3-4. (June 26, 2006). Available online at: http://www.dhs.gov/xlibrary/assets/hsac_minutes_06262006.pdf.