VIEWPOINT

Toward Inherently Secure and Resilient Societies

Brad Allenby[1]* and Jonathan Fink[2]

Recent years have seen a number of challenges to social stability and order, ranging from terrorist attacks and natural disasters to epidemics such as AIDS and SARS. Such challenges have generated specific policy responses, such as enhanced security at transportation hubs and planned deployment of a global tsunami detection network. However, the range of challenges and the practical impossibility of adequately addressing each in turn argue for adoption of a more comprehensive systems perspective. This should be based on the principle of enhancing social and economic resiliency as well as meeting security and emergency response needs and, to the extent possible, developing and implementing dual-use technologies that offer societal benefits even if anticipated disasters never occur.

Resiliency is defined as the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must. Developing enhanced resiliency is a rational strategy when the probability and specifics of a particular challenge are difficult to define. However, resiliency is not a global characteristic of a system; it can meaningfully be determined only with reference to an identified system and particular challenges. The Internet, for example, is characterized by a few hubs with high connectivity and an increasing number of other hubs with decreasing connectivity. Such scale-free networks are highly resistant to random failures, in that a substantial number of links can fail and still not affect the performance of the network as a whole. But such architectures are very vulnerable to a deliberate attack directed against the major hubs (*1*). For example, the September 11 attack on the World Trade Center only indirectly affected the Internet, which continued to function almost flawlessly (*2*); it would be much less resilient if directly attacked.

Frequently, a challenge will involve multiple scales, so that overall resiliency requires the ability to understand and take advantage of different initiatives at different levels. For example, designing a building that can be sealed against airborne pathogens is useful, and a number of such buildings in a downtown urban environment will enhance the urban area's overall resiliency against an attack. But designing building-level resilient systems will not substitute for an urban sensor system that enables early and accurate definition of an attack's parameters, nor for the emergency response effort that the city as a whole will need to mount. Analogously, there may be a number of opportunities in the "event life cycle" to implement resiliency strategies. One might invest in avoiding any event in the first place; creating long-term plans that reduce or mitigate threat; generating a warning in time to implement or adjust plans and reduce potential costs; mitigating the event as it occurs; or planning short-term responses and recovery or longer term recovery capabilities.

Some kinds of resiliency are primarily externalities, in that the protection gained provides almost no other benefits, whereas others are dual use and provide substantial economic benefits in addition to resiliency. For example, the communications systems provided to defense and national security organizations are commonly "hardened"; that is, additional technology provides protection against eavesdropping, destructive electromagnetic frequency pulses, and physical intrusion. This extra level of protection obviously adds cost to the system but not additional communications functionality (although the costs are presumably justified by the additional security obtained). In contrast, the creation of internal corporate intranets and support systems for virtual offices and telework capability, which diffuses information assets, can save firms money and make them more resilient against point attacks, as well as natural events such as epidemics (*3*, *4*). More broadly, when a resiliency option is less coupled to other functions, it can be more easily implemented, but it may not offer the additional benefits that strategic investments enhancing resiliency often do.

In general, a portfolio approach based on managing a number of varying risks should be the most efficient. Such an approach should seek to minimize not risk associated with individual events but risk across the social unit as a whole. The portfolio approach is also desirable given the difficulty of unambiguously defining risk and thus investments in resiliency. This ambiguity also serves as an argument for investment in dual-use options where possible—that is, investments that both enhance resilience against attack or disaster and provide additional economic, social, or environmental benefits. Not only are such dual-use technologies important because of resource limitations, but they enhance long-term security as well, for in the longer view a secure society involves innovation in strong infrastructure and social systems as well as in counterterrorism techniques and technologies. Fragile communities are more likely to be susceptible to disaster or attack and to disruption when such events occur and more likely to experience subsequent weakness and failure in the aftermath of an attack.

Network Organization and Urban Systems

Urban systems provide ideal laboratories for understanding resiliency and for developing dual-use technologies, practices, and systems that provide value even if no negative events occur. This is particularly true given accelerating urbanization: Developed countries are already highly urbanized, and the United Nations estimates that the urban populations of Africa, Asia, and Latin America will double over the next 30 years, from 1.9 billion in 2000 to 3.9 billion in 2030. At that point, over 60% of the world's population will live in cities (*5*). Moreover, the cultural, economic, and symbolic importance of urban systems to their societies makes them natural targets for deliberate violence; global transportation networks and high population density make them ideal centers for disease; and the concentration of economic assets and people that characterize them make them highly susceptible to damage from local natural disaster. But cities are not fragile. Indeed, throughout history they have often been destroyed—by fire, by disease, by nuclear attack, by earthquake, and by war—and yet, from 1100 to 1800 only 42 cities worldwide were abandoned after their destruction (*6*).

Cities also present challenging studies in resiliency because their nature is changing rapidly and fundamentally as information becomes an ever more important component of urban structure at all scales (*2*, *7*, *8*). Reliance on information infrastructures by other critical networks, such as transportation, financial, and corporate systems, is also rapidly accelerating (*9*, *10*); cities frequently form critical nodes where these networks intersect and interact. Moreover, the performance characteristics of these networks are also evolving rapidly. In telecommunications, for example, defined and fragile telephone networks have been replaced by Internet-based virtual networks that can be reconfigured and that monitor their own performance and structure and repair themselves in real time (*11*). Similarly, modern computing systems are being designed to con-

[1]Department of Civil and Environmental Engineering, [2]Office of Vice President for Research and Economic Affairs, Arizona State University, Tempe, AZ 85287–7205, USA.

*To whom correspondence should be addressed. E-mail: brad.allenby@asu.edu

tinuously monitor and tune their own performance; adapt to unpredictable conditions (making them resilient and not just engineered for redundancy); predict, prevent, and gracefully recover from failure; and provide safe, secure computing environments (*12*). It is not yet clear how these changes in demographics and information systems will affect the resiliency of urban systems. One immediate result has been increased interest in new tools that aggregate and display complex information patterns at the urban systems level, such as the immersive Decision Theater at Arizona State University (*13*, *14*). Such technologies not only facilitate coordinated emergency management and systemic responses to disasters, but enable better routine management of increasingly complex urban systems and can serve as important educational tools for city managers and the public. They are thus good examples of dual-use technology.

Network-Centric Organizations

The evolution of information-dense urban systems is paralleled by a trend in private firms toward network-centric organizational structures. This parallelism raises a number of questions, including how network-centric firms increase urban system resiliency or, alternatively, vulnerability; whether such firms are indeed more resilient and if so at what scales; and how corporate structure couples community, urban system, regional, and national patterns of social, technological, and economic resiliency. These are highly complex questions requiring further research, but some initial observations can be made.

It is elementary that physical dispersion of assets makes them less subject to point attack or localized disaster such as a tornado or earthquake. A decentralized workforce is also more resilient against a number of other disruptions, including disease (employees who are able to work from home run less risk of infection and help reduce the velocity with which infectious diseases can spread) (*4*). A dispersed workforce enhances resiliency in more subtle ways in addition to the obvious reduction in direct impact. The response to the September 11 attacks indicates that postevent stress and anxiety (the creation of which is a major purpose of many terrorist attacks) can be relieved substantially if arrangements are in place that enable dispersion of the workforce, especially to a home environment where they are both more comfortable and feel themselves less of a potential target (*15*). Ensuring that data and information are not located only in one area, but duplicated in facilities that would not be affected by the same local event, similarly helps protect against catastrophic loss. This was another lesson gained from the September 11 attack on the World Trade Center, where firms such as Lehman Brothers and Cantor Fitzgerald, which had established backup data facilities as part of their business continuity contingency plans, were able to rapidly resume operation (*2*).

But these new patterns of corporate structure have not arisen from concern about terrorism or from seeking resiliency of corporate performance in a risky world. Rather, they reflect economic pressures generated by today's globalized economy with its increasingly dispersed patterns of economic production and increased reliance on information as a critical input to economic activity and production of information as a valuable output (*9*, *16*, *17*). Stronger competition and a more rapidly changing operating environment lead firms and other institutions to adjust in many ways, such as implementing rapid cycle times, learning how to manage and use information networks, developing the ability to absorb and respond to complex information patterns, and emphasizing the knowledge of their workforce as an increasingly critical source of value. Institutional structures are shifting from rigid to more fluid and responsive network-centric organizational patterns, with value and productivity a function of how efficiently the firm can gather and manage knowledge (*2*, *16*).

Concomitantly, the critical infrastructure for many firms is shifting to a substantial degree from their physical assets, such as manufacturing facilities, to knowledge systems and networks and the underlying information and communications technology systems and infrastructure. The functionality that supports corporate, government, and other organizational structures, and most critical corporate data and operational information, now reside on corporate intranets, where they can be accessed from virtually anywhere. This is a costly and potentially disruptive transition in business models, involving substantial changes in many internal organizations such as human resources, real estate management, and information technology management, as well as raising legal, operational, and managerial challenges (*3*). Nonetheless, adoption of these technologies and techniques is driven by competitive pressure, particularly the need to manage costs and increase productivity. Thus, for example, some 30% of the managers at AT&T are completely "virtual" in that they have no assigned office in company-managed buildings, a corporate structure that produces $180 million in business benefits annually, primarily from productivity increases and real estate cost reduction (*4*). Other firms report similar financial benefits (*18*, *19*).

From the perspective of a city, policies that encourage a strong teleworking capability in local firms are ideal dual-use systems: They provide resiliency against disaster or attack, but many important ancillary benefits as well. An urban system with a large number of potential teleworkers can encourage working from home on bad air quality days, or during blizzards or other emergency conditions, or when unanticipated upsets in the traffic networks result in congestion. Moreover, an urban environment that encourages teleworking also provides a higher quality of life; AT&T's data indicate that 81% of its teleworkers name better balance between work and family as a substantial benefit of the practice (*4*). Additionally, some argue that by enabling people to work in their neighborhoods, telework can enhance a sense of community and neighborhood security (*20*).

Developing policies and tools to support implementation of such a dual-use technology is not easy. Novel issues, such as whether a city should invest at the margin in additional transportation infrastructure, such as wider roads, or information infrastructure, such as broadband to the home, are likely to arise. This question is complicated by how investments in information and communication technologies (ICT) interact with the overall evolution of information-dense urban structures. Moreover, the increased reliance on ICT systems and the Internet implied by this process can actually produce vulnerabilities, unless greater emphasis is placed on protecting information infrastructures, especially from deliberate physical or software attack to which they might be most vulnerable given their current structure (*3*). Accordingly, proper network design with hubs geographically separated (and critical ones perhaps duplicated), and network security sensitive to varying degrees of vulnerability of critical network components, including software functionality, should be part of any information and employee dispersion policy or national policy against terrorism.

This point has not been lost on governments. The United States, for example, has issued a series of executive orders and strategies intended to protect ICT infrastructure (*21*, *22*). But vulnerabilities, especially in the private sector, remain widespread, as recent well-reported compromises of consumer and employee data held by major firms indicate (*23*).

At the national scale, the implications of network-centric organizations are profound and only slowly being recognized. For example, reducing unnecessary transportation reduces demand for gasoline and thus enhances energy security. AT&T, for example, estimated that its telework/virtual office program even in 2000 was avoiding some 110 million unnecessary miles of driving per year, avoiding the consumption of more than 5 million gallons of gasoline (and emission of an estimated 50,000 tons of carbon dioxide) (*2*). It also seems likely that, if properly managed, a network-centric society might well be more equitable, more productive, and therefore perhaps less fragile in the face of challenge. Most obviously, many societies use only a small fraction of the intellectual capital available to them; some marginalize women, or noncitizens, but virtually all have relatively arbitrary ages beyond which they marginalize older workers, and most do not have mechanisms to include disabled workers in their economies. Network-centric

structures enable non–place-based access and temporary working arrangements, and cognitive capability built into network tools can facilitate economic integration of the disabled. This enhances not just the economic performance of society, but the quality of life of individuals involved; virtually all marginalized groups are highly interested in participating in the economy if they can and if the work can be structured to suit their requirements, which is precisely the flexibility the network-centric structure can provide. Thus, for example, seniors in the United States report a high interest in continuing to work flexibly (fewer hours, no required office, and no lengthy commutes) (*24*, *25*). On the demand side, the need for adequate knowledge workers will grow substantially as the baby boom generation retires (*25*), and management of pension shortfalls and old-age support policies might well be facilitated by the operational and social flexibility enabled by network-centric economic organization.

The range of ancillary effects discussed in this brief example illustrates the complexities and challenges of adopting the principle of resiliency as a policy and planning touchstone, as well as the potential value of dual-use tools and technologies. Understanding the interplay of these systems and how various investments and policy choices integrated into a resiliency portfolio can simultaneously enhance both security and economic and social stability and growth is not a trivial challenge, but the potential benefits argue strongly for such a course.

References

1. A. Barabasi, *Linked: The New Science of Networks* (Perseus Publishing, Cambridge, MA, 2002).
2. M. Moss, A. Townsend, in *Digital Infrastructures: Enabling Civil and Environmental Systems Through Information Technology*, R. Zimmerman, T. Horan, Eds. (Routledge, London, 2004), pages 141–152.
3. B. R. Allenby, J. Roitz, *Implementing the Knowledge Economy: The Theory and Practice of Telework* (Batten Institute, Darden Graduate School of Business, University of Virginia, Charlottesville, VA, 2003).
4. J. Roitz, B. Nanavati, G. Levy, "Lessons learned from the network-centric organization: 2004 AT&T employee telework results" (AT&T Telework White Paper, AT&T, Bedminster, NJ, 2005).
5. National Research Council, *Cities Transformed* (National Academy Press, Washington, DC, 2003).
6. L. J. Vale, T. J. Campanella, Eds., *The Resilient City* (Oxford Univ. Press, Oxford, 2005).
7. R. Zimmerman, T. Horan, Eds., *Digital Infrastructures: Enabling Civil and Environmental Systems Through Information Technology* (Routledge, London, 2004).
8. M. Amin, in *Digital Infrastructures: Enabling Civil and Environmental Systems Through Information Technology*, R. Zimmerman, T. Horan, Eds. (Routledge, London, 2004), pages 116–140.
9. M. Castells, *The Rise of the Network Society* (Blackwell Publishers, Oxford, 2000).
10. National Research Council, *Information Technology in the Service Society* (National Academy Press, Washington, DC, 1994).
11. AT&T Best Practices, Network Continuity Overview (2005); available at www.att.com/ndr/pdf/cpi_5181.pdf.
12. More information about autonomic computing is available at www-03.ibm.com/autonomic.
13. Arizona State University's Decision Theater Web site is available at http://dt.asu.edu/.
14. J. Fink, F. Steiner, C. Redman, N. Grimm, in *Earth Sciences in the Cities*, G. Heiken, R. Fakundiny, J. Sutter, Eds. (American Geophysical Union Special Publication Series 56), pages 413–426.
15. J. Roitz, personal communication.
16. P. Drucker, *Managing in the Next Society* (St. Martins Press, New York, 2002).
17. L. Edvinsson, M. S. Malone, *Intellectual Capital* (HarperCollins Publishers, New York, 1997).
18. Gartner Group, "Workplace transformation: A workplace imperative" (Report number R-11-0910, Gartner Group, New York, 2000).
19. AT&T Point of View: Remote Teleworking (2004); available at www.business.att.com/emea/english/whitepaper/pdf/remote_working_2004.pdf.
20. B. R. Allenby, D. J. Richards, *Environ. Qual. Manage.* **8**, 3 (2005).
21. U.S. White House, Executive Order 13231, Critical infrastructure protection in the information age, released 16 October 2001; available at www.whitehouse.gov/news/releases/2001/10/20011016-12.html.
22. U.S. White House, "The National Strategy to Secure Cyberspace," February 2003; available at www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.
23. "Information security: The leaky corporation," *The Economist*, 25 June 2005, pp. 57–58.
24. AARP, *Staying Ahead of the Curve: The AARP Work and Career Study* (AARP, Washington, DC, 2002).
25. The Conference Board, *Voices of Experience: Mature Workers in the Future Workforce* (The Conference Board, New York, 2002).

10.1126/science.1111534

VIEWPOINT

Social-Ecological Resilience to Coastal Disasters

W. Neil Adger,[1]* Terry P. Hughes,[2] Carl Folke,[3] Stephen R. Carpenter,[4] Johan Rockström[5]

Social and ecological vulnerability to disasters and outcomes of any particular extreme event are influenced by buildup or erosion of resilience both before and after disasters occur. Resilient social-ecological systems incorporate diverse mechanisms for living with, and learning from, change and unexpected shocks. Disaster management requires multilevel governance systems that can enhance the capacity to cope with uncertainty and surprise by mobilizing diverse sources of resilience.

Human populations are concentrated along coasts, and consequently coastal ecosystems are some of the most impacted and altered worldwide. These areas are also sensitive to many hazards and risks, from floods to disease epidemics. Here, we explore how a better understanding of the linkages between ecosystems and human societies can help to reduce vulnerability and enhance resilience of these linked systems in coastal areas. By resilience, we mean the capacity of linked social-ecological systems to absorb recurrent disturbances such as hurricanes or floods so as to retain essential structures, processes, and feedbacks (*1*, *2*). Resilience reflects the degree to which a complex adaptive system is capable of self-organization (versus lack of organization or organization forced by external factors) and the degree to which the system can build capacity for learning and adaptation (*3*, *4*).

Part of this capacity lies in the regenerative ability of ecosystems and their capability in the face of change to continue to deliver resources and ecosystem services that are essential for human livelihoods and societal development. The concept of resilience is a profound shift in traditional perspectives, which attempt to control changes in systems that are assumed to be stable, to a more realistic viewpoint aimed at sustaining and enhancing the capacity of social-ecological systems to adapt to uncertainty and surprise.

Coastal Hazards and Resilience

Natural hazards are an ongoing part of human history, and coping with them is a critical element of how resource use and human settlement have evolved (*5*, *6*). Globally, 1.2 billion people (23% of the world's population) live within 100 km of the coast (*7*), and 50% are likely to do so by 2030. These populations are exposed to specific hazards such as coastal flooding, tsunamis, hurricanes, and transmission of marine-related infectious diseases. For example, today an estimated 10 million people experience coastal flooding each year due to storm surges and landfall typhoons, and 50 million could be at risk by 2080 because of climate change and increasing population densities (*8*). More and more, adaptive responses will be required in coastal zones to cope with a plethora of similar hazards arising as a result of global environmental change (*9*).

Hazards in coastal areas often become disasters through the erosion of resilience, driven

[1]Tyndall Centre for Climate Change Research, School of Environmental Sciences, University of East Anglia, Norwich, NR4 7TJ, UK. [2]Centre for Coral Reef Biodiversity, School of Marine Biology and Aquaculture, James Cook University, Townsville QLD 4811, Australia. [3]Centre for Transdisciplinary Environmental Research and Department of Systems Ecology, Stockholm University, SE-10691 Stockholm, Sweden. [4]Center for Limnology, University of Wisconsin, Madison, WI 53706–1492, USA. [5]Stockholm Environment Institute, Box 2142, SE 103 14 Stockholm, Sweden.

*To whom correspondence should be addressed. E-mail: n.adger@uea.ac.uk