THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 11 NUMBER 6

December 2012
Resilience

Editorial Staff

Editors
Olivia Pacheco
Kendal Smith

JMU Coordinators
Ben Delp
Ken Newbold

Publisher
Imani Dunigan

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

GEORGE MASON UNIVERSITY
School of Law
CENTER
for
INFRASTRUCTURE PROTECTION
and
HOMELAND SECURITY

This month, *The CIP Report* focuses on resilience. A buzz word within the infrastructure protection community, our authors take a deeper look at the meaning of resilience and its usefulness as a practical concept in the face of human and man-made threats.

First, Debra van Opstal, Executive Director of the U.S. Resilience Project, discusses the importance of reslilience thinking in a world of increasing uncertainty, highlighting real-world examples such as cyber risks, climate volatility, water shortages, and interdependency failures. Next, Professor P.H. Longstaff advises us to avoid resilience "Kum Ba Yah," noting the tradeoffs that resilient infrastructure brings. Then, Scott Jackson and Timothy L.J. Ferris review the evolution of resilience from a notional concept into a practical idea.

This month's *Legal Insights* examines the importance of community resilience as a strategic policy initiaitve at the Federal, State, and local levels.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

The Resilience Imperative

by Debra van Opstal
Executive Director, U.S. Resilience Project
CIP/HS Fellow

The only thing we know with certainty is that the future is likely to be volatile and uncertain. Globalization, technological complexity, and interdependencies are new uncertainties and vulnerabilities. Who anticipated a Japanese tsunami that would cause a reactor meltdown with world-wide repercussions for the nuclear industry and global supply chains; or flooding in Thailand that would affect the global consumer electronics business for half a year; or an Icelandic volcano that would close trans-Atlantic air traffic for nearly a week?

Conventional risk management strategies often focus on identifying and prioritizing known risks and developing plans to mitigate them. That is still a necessary part of risk strategy, but not sufficient. In an era of turbulence, accurate prediction is impossible. And the velocity at which crises unfold makes every second of response time count.

Surviving uncertainty requires resilience—for companies, communities and countries. There are different definitions of resilience, but all have one common theme—the ability to sustain continuity in the face of adversity and to recover to a new (and potentially better) normal as quickly as possible. Resilience requires a different set of capabilities and competencies than conventional risk management:

- Resilient organizations focus on outcomes. They invest in agile and adaptive capabilities that allow them to minimize the impact of disruptive events, irrespective of risk trigger. Organizationally, they are replacing an orchestral model of crisis management—a set piece model that features a maestro, sectionals, and sheet music—with a jazz combo approach that enables flexible improvisation by accomplished practitioners.
- Resilient organizations build bridges between operational silos to increase connectivity, communication, and collaboration. In this interconnected world, risks do not respect silos; they cascade across them. There are no bright lines to demarcate specialized risk roles and responsibilities. Cyber security is often thought of as an IT problem, but in fact it

Critical Skills for Thriving in Uncertainty

Check Assumptions about the "knowns": Black swan is simply a metaphor for mental models. Europeans could not imagine that swans could be black until they went to Australia in 1697 and found them. Organizations often fail to challenge their assumptions about risks,even as the world is changing around them.

Maintain Constant Vigilance: To find the unexpected before it finds them, organizations need to be able to identify even weak signals of shifts and shocks that could impact their business model.

Factor in Velocity and Momentum: Bad things happen faster than good; reputations are gained in inches per year and lost in feet per second. The speed of response has to be matched to the speed of onset.

Maintain a Margin of Safety: Mark Twain noted that October is a particularly dangerous month. Other dangerous months are July, January, September, May, March, November, and so forth. A margin of safety is always needed to deal with the unexpected.

Develop and Sustain Operational Discipline: Benjamin Franklin said: Well done is better than well said. But, too often, when all has been said and done, more has been said than done.

Identify Critical Chokepoints: Humans can go three minutes without air, three days without water and three weeks without food. Understanding critical dependencies and how long we can go without them are critical to managing outcomes.

Adapted from Frederick Funston and Stephen Wagner, Surviving and Thriving in Uncertainty, *John Wiley & Sons, Inc., 2010.*

(Continued on Page 3)

Resilience Imperative *(Cont. from 2)*

spans manufacturing quality assurance, vendor management, logistical and warehouse security, anti-counterfeiting, IP protection, personnel and operational maintenance, upgrade and repair.

- Resilient organizations are agile, adaptive, risk intelligent, collaborative, and change-ready, exactly the qualities needed to be an innovative organization.

Why Resilience Will Matter Even More Going Forward

More turbulence is on the way. Think of the emerging risk landscape as a superhighway where risks can come from ahead, behind, or from either side. Managers who only look down their own lane are increasingly likely to be blindsided. The new classes of risk, which are cross-cutting, unpredictable, and potentially highly disruptive, include:

Cyber risks

Cyber attacks constitute a new frontier for most risk managers, with challenges ranging from cyber crime—estimated at tens of billions of dollars—to attacks on critical infrastructure, corporate databases, and national security systems. The fallout from a major cyber attack could be as lethal as a physical attack ,and surveys indicate that many (if not most) of us are unprepared.

Real world examples:

- ◆ Discovered in June of 2010, the Stuxnet computer worm, deemed the first cyber weapon of mass disruption, attacked specific industrial control systems, mostly in Iran, but provides a generic attack path to attack any control system in a critical infrastructure or manufacturing plant.
- ◆ The software security firm, McAfee, reported for the third quarter of 2012 that online financial fraud attacks have spread worldwide, that ransomware, which extorts money from its victims, became one of the fastest growing areas of cybercrime, that the number of malware specimens in the "zoo" topped 100 million, and that data breaches reached an all- time high.[1]

Climate Volatility

Hurricane Sandy simply validated the finding that: "Storms are happening in places they never happened before, at intensities they have never reached before and at time of the year when they did not used to happen."[2] No one is immune from the effects of climate volatility.

Real-world examples:

- ◆ Current estimates (still guesstimates) put losses for Hurricane Sandy between $50-80 billion.
- ◆ Research by Munich Re indicates that the number of weather-related disasters has increased by a factor of five over the past three decades, and grown fastest in North America.[3]
- ◆ Climate volatility is beginning to show up as a material risk in corporate filings with the Securities and Exchange Commission.[4]

Water Shortages

Although related to climate volatility, water shortages create a different set of risks. Duke Energy CEO, Jim Rogers, described water as "the new oil."[5] To put it in perspective: "If we could compress all the water on the planet into a single gallon, four ounces would be fresh water. Of those four ounces, two drops would be accessible to humanity, of which one drop is already in use."[6] And the competition for access to water among municipalities, farmers, industrial and power suppliers is growing—and setting up some contetious choices.

Real-world examples:

- ◆ More than one-third of the world's population—roughly 2.4 billion people—live in water-stressed countries and by 2025, that number is expected

(Continued on Page 10)

[1] *McAFee Threat Report*, Third Quarter (2012) available here.

[2] Ben Berkowitz, "Extreme Weather Batters the Insurance Industry," Reuters (February 9, 2011) available here.

[3] Munich Re, "Severe Weather in North America" (October 2012) available here.

[4] David Gardiner & Associates, "Physical Risks from Climate Change," Oxfam America, Calvert Investments and Ceres (May 2012).

[5] Ken Silverstein, "Water Shortage May Leave Energy Producers Dying of Thirst," Forbes (May 3, 2012) available here..

[6] "Counting the Cost of Water," O2 Environmental Inc. (August 26, 2007) available here.

Avoiding Resilience "Kum Ba Yah" Recognizing the Tradeoffs Before They Become Surprises

by P. H. Longstaff*

A week after superstorm Sandy hit the Northeast coast of the US the *New York Times* published a contributor Op Ed that suggested that maybe it is time to stop pretending we can stop all potential (and increasingly likely) disasters.[1] Dangers from big storms and big cyber attacks are for real and, at least for the moment, we cannot stop them. We can, and will, use our increasingly sophisticated surveillance capabilities to get an early warning that can limit the damage. But the big political message from that disaster was that people need to be able to bounce back if the danger cannot be prevented. And they want to bounce back quickly. They want their infrastructure to be resilient. Nonetheless, it is crucial to remember that resilience comes with costs and now would be the time to acknowledge them. We do not need "Resilience Kum Ba Yah" for infrastructure or anything else.

Readers who know me may be surprised that I would write such a thing. I have been talking about using resilience concepts to find new ways to manage uncertainty for a few years now.[2] I have tried to explain resilience to some very skeptical audiences—many of whom were sure it was just the buzzword de jour. I remain convinced that resilience is an important capability in many systems: from materials science to ecology and from individuals to organizations. The similarities in its operation across those systems gives us clues about things we can try in the systems we need to manage through times of high uncertainty. The similarities also give us clues about tradeoffs we may need to deliberately acknowledge and not wait for those tradeoffs to surprise us.

This would not be the first time that over-exuberance about a public policy has come back to bite us. When the Internet was young it inspired rapturous predictions of how it would save the world. A colleague of mine called it "Internet Kum Ba Yah,"[3] referring to the wonderful African American spiritual song that has inspired and entranced generations. These Internet supporters ignored any potential dark sides for unlimited world-wide communication and they convinced policy-makers of their visions. We are, of course, living with those dark sides now. Let's learn from this. Resilience does not have all the answers and it will demand some very real and very difficult tradeoffs.

I want to bring two of those tradeoffs to your attention because I think they will be important for resilient infrastructures, for both engineering and the policy-making. Both of these ideas challenge some of our most basic assumptions so I expect you to be saying "No way!" when you see them. They are efficiency and blame.

Efficiency as the Enemy of Resiliency

So we start by defining "efficiency" for purposes of this discussion. It is a strategy for getting the most output from the least input to the system. It means, for example, getting the most bandwidth or electricity to consumers at the lowest cost. Typical ways of achieving efficiency in any system include getting really good at one thing (adapting totally to your current environment), getting all your resources from one place so you can streamline your supply chain, and getting rid of any costs

(Continued on Page 5)

[1] Andrew Zolli, "Learning to Bounce Back," *New York Times*, November 3, 2012. available here.

[2] See, e.g., Longstaff, P., *Security, Resilience, and Communication in Unpredictable Environments Such As Terrorism, Natural Disasters, and Complex Technology*, Harvard University Program for Information Resources Policy, November 2005, available here; Longstaff, P. et. al., 2010, "Building Resilient Communities: A Preliminary Framework for Assessment." *Homeland Security Affairs VI,* no. 3 available here.

[3] "Kum Ba Yah" is usually translated as "come by here."

Avoiding Kum Ba Yah *(Cont. from 4)*

that will not contribute to your laser-like focus. And all that works for many industries until they find themselves facing new uncertainty. And it might have worked for the infrastructure industries that had been operating without much change for years, except that they were also supposed to deliver their services even under high uncertainty. And in the 90's policy-makers gave them some uncertainty in order to make them efficient.

Competition (another concept that got the Kum Ba Yah treatment a few years ago) was supposed to make infrastructure industries more efficient (and cheaper) and in many ways it did. But the tradeoffs were not acknowledged. The "most output for the least input" meant that investments in things that were all cost and no income (like redundancy for important parts of the system) were made only at levels that could be justified for predictable disasters. That works as long as there are only predicted disasters. When something bigger or weirder happens, the same policy-makers who demanded more efficiency will now want to know why there are not more back-up systems.[4]

In many systems, resiliency is enhanced when it is made up of many small individuals that reproduce quickly. In technical systems, this is analogous to distributed service hubs that can get back in business relatively quickly because they are not dependent on resources from distant places. They have the freedom to improvise with the resources they have on hand. They are not tightly coupled to a larger network. This is almost certainly not as efficient as building one or several very large hubs. But a distributed system will bounce back quicker for local populations because it does not require rebuilding all the coordination functions necessary for putting the larger organizations back together.

Organizations often try to get efficiency by replacing humans with machines. These machines will be very efficient at delivering a service under the conditions they were designed for, but are not capable of improvisation when there is a change in conditions. If they are not backed up with some sort of redundant system they may fail entirely. You can also get more efficiency by training employees for very specific jobs they can do very quickly under typical conditions. But when conditions are not typical, managers will have little flexibility to improvise staffing levels. Having employees cross-trained to do several jobs is expensive and takes time away from what they are supposed to accomplish.

These tradeoffs between resilience and efficiency are seldom acknowledged in the planning process. Meeting budget or output levels often seems more important. The potential problems are left unacknowledged, waiting to surprise everyone. But these deeper problems are not dealt with in the typical after-incident analysis, and a human is generally found to blame—because they are usually easy to find. But this, too, will reduce resilience.

The Blame Game can make you less resilient

Eric Hollnagel has studied reliability in many critical technical and human systems.[5] He has written extensively on the role that blame plays in these systems. He suggests a balance between accountability and learning. He admits that setting out all unacceptable behavior in advance (particularly in systems with high uncertainty) is not possible and so there must be a mechanism that is perceived as relevant and fair for making these decisions. He suggests building a "Just Culture" that balances concerns for fairness with

(Continued on Page 12)

[4] For more on the tradeoff between efficiency and redundancy in various systems, see, Hollnagel, *The ETTO Principle: Efficiency-Thoroughness Tradeoff: Why Things That Go Right Sometimes Go Wrong*, Ashgate Publishing: Surrey and Burlington VT (2009); Bobbi Low, Elinor Ostrom, Carl Simon, and James Wilson, "Redundancy and Diversity: Do They Influence Optimal Management?" in *Navigating Social-Ecological Systems: Building Resilience For Complexity and Change*, eds., Fikret Berkes, Johan Colding, and Carl Folke, Cambridge,UK and New York: Cambridge University Press (2003) pp. 83-114.

[5] Eric Hollnagel, *Behind Human Error*, Woods, et al., eds., Ashgate Publishing: Surrey, UK and Burlington VT USA, (2010). See also, Hollnagel, *The ETTO Principle: Efficiency-Thoroughness Tradeoff: Why Things That Go Right Sometimes Go Wrong*, Ashgate Publishing: Surrey and Burlington VT (2009).

Infrastructure Resilience: Past, Present, and Future

by Scott Jackson and Timothy L. J. Ferris

This article reviews the concept of resilience, especially when applied to civil infrastructures, how this concept gained recognition as something of importance, and how it is evolving from a notion to a practical idea.

Phase 1: The Early Days

Initial interest in resilience was stimulated primarily by the fact that policy makers realized that protecting our infrastructure from all possible threats, man-made and natural, was just unreasonable. First of all, the cost of doing so would be astronomical. Secondly, the more important priority is to maintain the continuity of essential life resources: food, water, power, ect. So the question became: is this possible even if key assets are lost? Hence, the early thinkers considered it important to make a distinction between resilience and protection. In 2007, a group at George Mason University published the report *Critical Thinking: Moving From Infrastructure Protection to Infrastructure Resilience* addressing this issue,[1] and the 2010 White House *National Security Strategy* reinforced the importance of resilience on a national level.[2]

Another group responsible for much of the seminal thinking on resilience are the authors of the book *Resilience Engineering: Concepts and Precepts* by Hollnagel et al (2006).[3] These authors saw resilience as primarily an organizational concept. ASIS International also published a standard devoted entirely to organizational resilience which holds that the purpose of the organization is to protect its physical assets.[4] As the Phase 2 discussion will show, later researchers began to think of resilience in a "total systems" context to include organizations as well as physical assets, such as dams, railroads, and so forth.

Although during Phase 1 there were many efforts to define resilience, the National Resilience Coalition has adopted the following definition which contains all of the essential elements of resilience: "Resilience is the ability to prepare and plan for, absorb or mitigate, recover from, or more successfully adapt to actual or potential adverse events."[5] One of the features of this definition is the pro-active aspect of resilience reflected in the words "prepare and plan for." Some writers had previously considered resilience to be only a reactive concept that applied after an encounter with a threat. So this definition broadens the scope of resilience to include the pre-encounter anticipation of the threat. Hollnagel et al agree with this aspect. We have concluded, however, that even this definition is simplistic and cannot accurately reflect all the threat and domain scenarios that may exist. We suggest that the individual wishing to

(Continued on Page 7)

[1] In *CIP Program Discussion Paper Series*, George Mason University School of Law (2007).

[2] *National Security Strategy*, The White House (2010), available here.; *see also* Wayne E. Boone and Steven D. Hart, *Full Spectrum Resilience*. The Infrastructure Security Partnership (TISP) (2012 unpaginated), available here., for a more comprehensive summary of the history of resilience as a subject of national importance.

[3] Erik Hollnagel, David D. Woods, and Nancy Leveson, eds., *Resilience Engineering: Concepts and Precepts*. Aldershot, UK: Ashgate Publishing Limited (2006).

[4] *Organisational Resilience: Secuirty, Preparedness, and Continuity Management Systems--Requirements With Guidance for Use* (2009).

[5] Available here; *see also* Stephen E. Flynn and Sean P. Burke, Powering America's Energy Resilience, 3, Center for National Policy (May 2012) available here.

Infrastructure Resilience *(Cont. from 6)*

analyze these scenarios should parse this definition to reflect the scenarios of interest. One of the issues to be resolved during the first phase was the difference between resilience and risk. It was agreed that resilience and risk are different but related concepts. Resilience has to do with the ability of a system to recover from a disruption, while risk is the ability to avoid a catastrophic failure.

Abstract Principles and Dominant Characteristics

Principle	Dominant Characteristics
Absorption	System capable of absorbing design threat level
Physical Redundancy	System consists of two or more identical and independent branches
Functional Redundancy	System consists of two or more different and independent branches
Layered Defense	System does not have a single point of failure
Human in the Loop	System has human elements where needed
Reduce Complexity	System capable of reducing the number of elements, interfaces, and/or variability among its elements
Reorganization	System capable of restructuring itself in the face of a threat
Repairability	System capable of repairing itself following a disruption
Localized Capacity	Individual elements of a system are capable of independent operation following failure of other elements
Loose Coupling	System resistant to cascading failure by slack and delays at the nodes
Drift Correction	System capable of detecting approaching threat or hidden flaws and performing corrective action
Neutral State	System capable of entering neutral state to allow decisions to be made
Inter-node Interaction	System has connections among all its nodes
Reduce Hidden Interactions	System capable of detecting undesirable interactions among its elements

Phase 2: Recent Developments

Phase 2 has seen the concept of resilience evolve from a notional idea to a subject of expanded scholarly interest with publications in peer-reviewed journals. Typical among these are those by Yacov Haimes.[6] In addition, Jackson and Ferris[7] (2012) have evaluated a set of abstract principles extracted from the literature including some suggested by Hollnagel et al, above.

Abstract principles are mental concepts from which concrete solutions may be developed. Abstract principles cannot be measured, but concrete solutions can be measured, modeled, and simulated. Both abstract principles and concrete solutions are characterized by dominant characteristics that are summarized in the table below. The systems of interest in this phase are total systems including both organizations and physical assets.

Jackson and Ferris also determined that these principles cannot be implemented singly but rather they must be implemented in appropate combinations to achieve their goals. Additionally, these principles have their own vulnerabilities and limits that must be analyzed before they are implemented.

What can a system developer do with all these principles? In short, he or she can develop concrete solutions from them and then evaluate the concrete solutions via the models suggested by Haimes below. In short, there is no way to know whether one principle is better than another; that comparison can only be made at the concrete solution level. The concrete solutions must, of course, possess the same dominant characteristics as the abstract principle. The discussion below will show that even that is not easy.

Phase 3 – The Road Ahead

Haimes has pointed to some of the

(Continued on Page 13)

[6] *See* Yacov Haimes, *Homeland Security Preparedness: Balancing Protection with Resilience in Emergent Systems* in Systems Engineering, 11 (4):287-308 (2008); Haimes, *On the Definition of Resilience in Systems,* in Risk Analysis, 29 (43):498-501 (2009)*;* and Haimes, *Modelling Complex Systems of Systems with Phantom System Models, in* Systems Engineering, 15 (3):333-346 (2012).

[7] *See* Scott Jackson and Timothy Ferris, *Resilience Principles for Engineered Systems*, in Systems Engineering, DOI 10.1002/sys21228 (2012).

Legal Insights

The Importance of Supporting Community Resilience

by Manal Farooq, CIP/HS Research Assistant

Nearly a month after Hurricane Sandy's assault on the East Coast, we are once again reminded of the importance of response and recovery after a disaster occurs. The unpredictability of man-made threats and natural disasters are unavoidable. We need to recognize the importance of fostering resilience at not only the Federal and State levels, but also in our local communities and organizations. In the wake of a disastrous event, resources become limited and citizens turn to their communities for help. Thus, it is becoming increasingly important to enhance community resilience in efforts to reduce recovery time after a disaster strikes. Resilience has become a strategic policy issue which has been incorporated at the Federal, State, and local levels. DHS has made efforts to integrate community resilience into its more recent policy documents.

The *Quadrennial Homeland Security Review (QHSR) Report*, released in February 2010, identifies resilience as one of its three essential concepts and It defines it as "*foster[ing] individual, community, and system robustness, adaptability, and capacity for rapid recovery.*"[1] The report goes on to identify Ensuring Resilience to Disasters as one of its five core missions. Resilience initiatives that advanced out of the QHSR's missions provide the means needed to invest in the continuity of essential national and community based functions.[2]

Presidential Decision Directive (PPD) 8, *National Preparedness* also discusses ways to strengthen "the security and resilience of the United States…."[3] It calls for the development of a National Preparedness Goal (NPG) which emphasizes five mission areas: prevention, protection, mitigation, response, and recovery.[4] The first NPG, published in September 2011, calls for sustaining resilient systems, communities, and critical infrastructure support.[5]

Although a August 2012 report released by the Congressional Research Service suggests that DHS has always given importance to community resilience in its policy documents, how can we make certain that local communities and organizations—all of which are part of an effective and operative society—are resilient?[6]

The Community Resilience Task Force (CRTF) of the Homeland Security Advisory Council (HSAC) was formed to provide the DHS Secretary with recommendations that facilitate creating and implementing community-based resilience policies and programs throughout the Nation.[7] Although many relevant activities are already underway, in June 2009, CRTF reported that "those activities are rarely linked explicitly to resilience."[8] CRTF continues to urge for a more clear relationship between resilience and homeland security efforts.

(Continued on Page 9)

[1] The Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, (Washington, DC: Office of the Secretary, February 2010), at ix.

[2] Ibid, at x.

[3] President Barak Obama, *Presidential Policy Directive/ PPD-8: National Preparedness,* (Washington, DC: The White House, March 30, 2011), available here. Note: PPD-8 replaced the 2003 Homeland Security Directive (HSPD) 8.

[4] Ibid.

[5] John D. Moteff, Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress, (Washington, DC: Congressional Research Service, August 23, 2012), available here.

[6] Ibid, at 19.

[7] Ibid, at 14.

[8] Ibid.

Legal Insights *(Cont. from 8)*

In addition to the formation of the CRTF, DHS, in its 2012-2016 *Strategic Plan*, elaborates on the QHSR's mission of *Ensuring Resilience to Disasters* by incorporating the Federal Emergency Management Agency's (FEMA) "whole community" approach. FEMA's December 2011 publication defines "whole community" approach[9] as a "means by which residents, emergency management practitioners, organizational and community leaders, and government officials can collectively understand and assess the needs of their respective communities and determine the best ways to organize and strengthen their assets, capacities, and interests."[10] An objective of the QHSR's *Ensuring Resilience to Disasters* mission, as outlined in the DHS *Strategic Plan*, is to improve community capacity to endure disasters by mitigating all threats and risks. DHS recognizes the importance of the "whole community" approach as a foundation for achieving a more resilient Nation. DHS also emphasizes the need to establish and maintain fundamental capabilities at the community and local levels in order to improve coordination and unity of effort as it relates to the Nation's ability to adapt and recover rapidly.[11]

Despite the vague and minimum efforts to support it, resilience has been programmatically incorporated at the community level. FEMA has managed a number of programs which focus on planning, developing, responding, and recovering from disastrous events, while addressing community resilience. For instance, the State Homeland Security Grant Program (SHSGP) and the Urban Areas Security Initiative (UASI) are mainly responsible for supporting the preparedness activities of State and local communities. Moreover, the Citizen Corps Councils support citizen preparedness by public and private means. The Voluntary Private Sector Preparedness Program (PS-Prep) is another program which touches upon resilience. Though it is a voluntary program, it promotes disaster and emergency management, and business continuity by offering accreditation to the private sector.[12]

While several of the current DHS programs take resilience into consideration, Federal and State governments need to expand dialogue with local communities to create more solid policies and programs which promote community resilience. Community resilience provides a framework for local communities to participate in preparing for and responding to a wide variety of risks and threats. With unforeseen man-made threats and natural disasters, it is becoming increasingly important to develop more resilient communities of responsible and informed citizens who are able to prepare for and respond to disasters in efforts to reduce long recovery periods.❖

[9] The Department of Homeland Security, *Department of Homeland Security Strategic Plan, Fiscal Years 2012-2016*, (Washington, DC: Office of the Secretary, February 2012), available here.

[10] The Federal Emergency Management Agency, *A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action*, (Washington, DC, December 2011), FDOC 104-008-1, at 3.

[11] The Department of Homeland Security, *Department of Homeland Security Strategic Plan, Fiscal Years 2012-2016*, see above, at 15, 17.

[12] John D. Moteff, *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*, see above, programs listed out at 15-17.

Resilience Imperative *(Cont. from 3)*

to rise to two-thirds. [7]

- A business-as-usual water demand scenario will outstrip supply by 40%, potentially putting $63 trillion of global GDP at risk.[8]
- In 2011, a decision by the Lower Colorado River Authority not to sell water to a large proposed coal plant in southeast Texas was seen as a harbinger. According to the head of the Electric Reliability Council of Texas, Trip Doggett: "We normally think of a plant as being a fairly sure bet once they get their air permit and their interconnection agreement with the transmission company. But we're beginning to believe that we probably need to add their water availability to that list."[9] In fact, water could be a principal stumbling block to the clean energy economy.

Affordability and Access to Strategic Minerals

New technologies and engineered materials create the prospect for rapid increases in demand for minerals. Intel estimates that computer chips, which used 11 mineral-derived elements in the 1980s and 15 elements in the 1990s, will incorporate up to 60 elements in the coming years.[10] Mobile phones, computers, electric vehicles, and green energy markets will continue to drive demand for strategic minerals—and in 2011, the EU identified critical shortages for 14 of these minerals.[11] But, even where resources are abundant, long term materials strategies may still be necessary. According to researchers at Cal Tech, China now uses 40% of the world's copper, compared to just 6% in 2000. If their current growth demand continues, China will need the equivalent of the world's current copper production by 2018. While ample resources exist, it may not be possible to increase product fast enough to meet demand.[12]

Real-world example:

- In August of 2012, citing environmental and health concerns from its mining activities, China announced that it would shutter one third of its 23 rare earth mines and one half of its 99 rare earth smelters, and reduce its rare earth exports by one fifth. Media reports indicated that China will establish a trading platform and pricing index to impose tighter controls on the rare earth metals market.[13]

Critical Interdependencies and Failure Paths

"Today's new reality is marked by hyperconnectivity, hypertransparency and ever deepening interdependencies."[14] Disruptions can cascade across geographies (the 1977 NY blackout began in Ohio); across infrastructures (power outages affect communications and vice versa), and across industries.

Risk failures also cascade between the public and private sectors. Private risk failures create public disasters. The 2007 mortgage crisis triggered a global credit crisis and recession. The 2010 malfunction of a blowout control valve in the Gulf of Mexico created economic, environmental, and health effects. In the same way, risk failures in the public sector can affect the private sector's ability to conduct business. For example, the failure to contain the 2009 H1N1 outbreak in Mexico sparked the first globally declared pandemic since 1968.

Real World Example:

- The devastating impact of an attack on the power grid has been likened to a cyber Pearl Harbor. What has received less attention is that solar activity

(Continued on Page 11)

[7] Morrison et al., *Water Scarcity and Climate Change: Growing Risks for Businesses and Investors*, Pacific Institute (February 2009) available here.

[8] "A Drought in Your Portfolio: Are Global Companies Responding To Water Scarcity?" *EIRIS Water Risk Report,* p. 1 (June 2011) available here.

[9] Kate Galbraith, "Electric Grid in Texas Faces Multiple Challenges," *New York Times* (December 22, 2011) available here.

[10] Roderick G. Eggert, "Critical Minerals and Emerging Technologies," *Issues in Science and Technology*, National Academy of Sciences (2010) available here.

[11] Available here.

[12] *Materials for Sustainable Energy Applications*, Resnick Institute Report, Caltech, 14 (September 2011) available here.

[13] "China's Rare Earth Supply to Get Even Rarer (and Why that Should Worry You)," *Smart Grid News.Com* (August 9,2012) available here.

[14] Dov Seidman, *The HOW Report: New Metrics for a New Reality: Rethinking the Source of Resiliency, Innovation, and Growth*, LRN (2012) available here.

Resilience Imperative *(Cont. from 10)*

could cause a similar impact. Solar activity flares every 11 years with the solar maximum approaching in December 2012 through 2013. A strong geo-magnetic storm could equate to a "Space Weather Katrina" according to the National Academy of Sciences. Such a storm could cause $1-2 trillion in losses, with a recovery time of four to ten years.[15]

The bottom line is that it is no longer possible to anticipate, plan for or prevent every disruption. Fortunately, a resilience strategy makes that unnecessary. Although each of these emerging risks poses special mitigation challenges, there are similarities and synergies of solution in the processes, capabilities, and tools required for continuity, response, and recovery. As Chad Holliday, the former CEO of DuPont noted: His company almost never got the crisis they prepared and practiced for. But, with resilient processes and people, they were able to manage whatever crises came their way.[16] In a world of expanding risks, resilience is an imperative for both competiveness and security. The ability to survive and thrive in turbulence is becoming a key competitive differentiator for companies, communities, and countries.❖

[15] Rik Myslewski, "NASA: Civilization Will End in 2013 (Possibly)," *The A Register* (June 16, 2010) available here.

[16] DuPont Chairman Charles O. Holliday, Jr., Speaks About Enterprise Resilience at the National Press Club" (June 25, 2007) video available here.

CALL FOR PAPERS

THE 2013 CRITICAL INFRASTRUCTURE SYMPOSIUM

"Advancing Full Spectrum Resilience" • April 15-16 • Thayer Hotel, West Point, New York

Hosted By: The Infrastructure Security Partnership, Society of American Military Engineers, the U.S. Army Corps of Engineers Engineer
Research and Development Center, and the U.S. Military Academy at West Point

For additional information please click here.

Avoiding Kum Ba Yah *(Cont. from 5)*

organizational cohesion, loyalty, and safety. This balance will be different in each organization and the balance will probably have to be reexamined periodically.[6] In many organizations it will make sense for the specifics of this new culture to emerge over time as it adapts to changing uncertainties. Imposing something from the top down that does not allow for adaptability will only make the organization more brittle and vulnerable to things like failures that cascade throughout the system.

A reexamination of the Blame Game in critical infrastructures is absolutely essential if we are to give people who must make them work what they need: the flexibility to respond. Unfortunately, when an event like a natural disaster or a terrorist attack becomes political (and they always do) much of the information about what actually happened may become closely guarded by individuals who want to protect those who may be blamed. This can have tragic consequences during and after the disaster because it is not possible to manage any kind of system unless we receive accurate feedback about what is happening in the system and to the system. If the "surprises" that occur in these systems are concealed because they are seen as "failures" of the system or "errors" of the person in charge, the system cannot learn or adapt to the changes that the surprise makes obvious.[7]

Some readers will be surprised to learn that it is often difficult (or impossible) to pinpoint one cause for surprises or malfunctions in complex technical or human systems. A lengthy investigation by independent parties is likely to come up with a list of things that contributed to the incident. Many of these things will indicate problems with the system and not with individuals in the system. But if it is the system, then is the person in charge of the system at fault? Who is accountable?

We often demand accountability because we think it will improve performance. But if the "… accounting is perceived as illegitimate,…intrusive, insulting, or ignorant of the real work, then the benefits of accountability will vanish or backfire. Effects include decline in motivation, excessive stress, and attitude polarization…."[8] They also include defensive posturing, obfuscation of information, protectionism, and mute reporting systems.[9] Clearly, the rules for accountability must be understood by everyone and perceived as fair in order to accomplish improved performance. And it may be important to distinguish accountability (the ability to account for or explain things) from blameworthy actions that result in some form of punishment. It has been observed that accountability can be seen as forward-looking while blame is backward-looking.[10] Error in complex systems is inevitable, blame is not. None of this is to say that we should not punish people who are negligent, lazy, or corrupt. These people do not help organizations learn or become more adaptable.

And so….

A conversation about the role of efficiency and blame in resilient systems should have very high priority as we prepare for the uncertainties we know we will be facing. This should take place at all scales of our infrastructures, from the local to the global. It will not be an easy conversation because it challenges some of our most closely held beliefs. We will not be singing Kum Ba Yah. ❖

**P. H. Longstaff is Professor of Television, Radio, and Film at the S. I. Newhouse School of Public Communications, Syracuse University, and a Research Associate at Harvard University's Program on Information Resources Policy.*

[6] Ibid., at pp. 233-234.

[7] Longstaff, P.H., "Is the Blame Game Making Us Less Resilient? A Reexamination of Blame Allocation in Systems with High Uncertainty," *Proceedings of the First International Symposium on Societal Resilience*, Homeland Security Studies and Analysis Institute, Washington, DC, 2012.

[8] Eric Hollnagel, *Behind Human Error*, Woods, et al., eds., Ashgate Publishing: Surrey, UK and Burlington VT USA, (2010), pp. 225-26.

[9] Ibid, at 225.

[10] Ibid, at 233.

Infrastructure Resilience *(Cont. from 7)*

challenges which future research can tackle. First of all, he tells us that resilience is "non-deterministic."[8] Non-deterministic situations are uglier than probabilistic or deterministic situations, in that the non-deterministic situation does not enable us to describe outcome conditions with meaningful probabilities. The most likely reason is that the system in a non-deterministic situation is sufficiently complex that it is not clear how any description of input conditions described at a reasonable level of complexity would map to actual impacts on the system, and therefore to outcomes either deterministic or probabilistic.

Haimes tells us that there are simply too many unknowns to determine exactly how well a system will recover from a disruption. He refers to these unknowns as state variables. First of all there is the time state; that is, when did the disruption occur? Then there is the system state. What was the state of the system at the time of the disruption, and what was the extent of the disruption, and so forth? Then there is the decision state; what decisions will the system operator make? In short, the system developer cannot evaluate the resilience of a system over all possible states. He or she can only model the system for selected states and make a judgment based on that set of cases.

Another challenge that Haimes presents to us is to determine the resilience of a system of systems. A system of systems is a collection of systems, such as infrastructure systems, that must work together to achieve a common goal, namely, to provide the products and services that a society needs. The problem is that all these systems, such as fire and police departments, water, electricity and telephone networks etc., have been separately developed so that how they work together in a new emergency situation is completely unknown. The resulting behavior in systems terminology is known as emergent behavior. Haimes describes the trial and error method of modeling such systems. Creating a suitable model is another challenge for the future researcher in resilience.

Probably the greatest challenge in resilience is finding the money to implement the concrete solutions recommended. It must be recognized that some concrete solutions are amazingly cheap since they are mostly procedural. Standardization of radio frequencies between fire departments, police departments, etc. is one of the cheap steps identified by the 9/11 Commission. There are political hurdles at a national level, but local implementation may be an option. Boone and Hart provide a plan on how a doctrine could be developed to implement resilience.[9]

Then there are the high cost items, such as finding a solution to the damage that would be caused by a break in the Sacramento Delta levee. Such a break is considered a near certainty. The simple rule is that if the predicted damage costs more than the preventive measures, then it is worth it. Nevertheless, finding the money is still a challenge.

Summary

In short, the study of resilience has come a long way from the concepts identified by Hollnagel et al and others. Much work has been done in identifying the principles and the challenges associated with them. The road ahead is to address the challenges. ❖

[8] Haimes, *Modelling Complex Systems of Systems with Phantom System Models*, in Systems Engineering, 15 (3):333-346 (2012).

[9] Boone and Hart (2012, unpaginated).

The Center for Infrastructure Protection and Homeland Security Presents:

Fatigue Risk Management in Aviation Operations

The Ongoing Fight for Alertness and Safety

The symposium will equip attendees with the knowledge and approaches necessary to effectviely fight fatigue in the operational setting. The human physiology of fatigue and the hazards it represents in the workplace will be explored, along with effective methods and tools to conduct fatigue risk management, mitigate fatigue's negative effects and enhance public safety.

The One Day Session will be held on

January 31, 2013

For more information on Registration and the Agenda **click here**.

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1