Beyond the Storms: Strengthening Preparedness, Response, & Resilience in the 21st Century

Dane S. Egli

Johns Hopkins University, dane.egli@jhupl.edu

Follow this and additional works at: <https://digitalcommons.usf.edu/jss>
pp. 32-45

Recommended Citation

Egli, Dane S.. "Beyond the Storms: Strengthening Preparedness, Response, & Resilience in the 21st Century." *Journal of Strategic Security* 6, no. 2 (2013) : 32-45.

DOI: <http://dx.doi.org/10.5038/1944-0472.6.2.3>

Available at: <https://digitalcommons.usf.edu/jss/vol6/iss2/3>

This Article is brought to you for free and open access by the Open Access Journals at Digital Commons @ University of South Florida. It has been accepted for inclusion in Journal of Strategic Security by an authorized editor of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.

Beyond the Storms: Strengthening Preparedness, Response, & Resilience in the 21st Century

Abstract

Looking *Beyond the Storms* of major events and reactionary tendencies to prevent future disasters—and continuing to fix things—the author introduces a fresh assessment in the wake of Superstorm Sandy, the vexing challenge of domestic shootings, and a persistent nationwide drought. This paper offers a refreshing perspective on the need for transformational and innovative thinking on preparedness, response, and resilience, as well as disaster management. Against the backdrop of 9-11 terrorist attacks and natural disasters such as hurricanes Katrina, Irene, and Sandy, this paper highlights that we—as homeland security planners and policymakers—must look beyond the immediate demands of grant proposals and a narrow focus on “prevention” and “protection” to a systemic analysis of “mitigation, response, and recovery”—based upon required functions and capabilities. It asserts the need for change from spending scarce dollars to prevent that which is inevitable and nervously trying to protect physical locations—in an environment of growing complexity and uncertainty—to a posture that integrates resilience as an active virtue in all elements of the homeland security enterprise. There is a sense of urgency that challenges leaders to understand the strategic imperatives and unique opportunities in building all-hazards community resilience.

Introduction

There is no safe harbor to avoid the impact of catastrophic events – “physical” disasters, such as extreme weather, earthquakes, and terrorism; or those that are “virtual” such as chemicals, infectious diseases, money, and electrons – and their direct or indirect consequences on the homeland. We face rapidly changing times, globally and nationally, marked by complexities and uncertainties that force us to make difficult decisions about homeland security and community preparedness.¹ This article suggests a new approach that leverages whole-of-government and private-sector capabilities to systematically strengthen preparedness, response and resilience.

The destabilizing impact of recent disasters has provoked a reactionary posture that is not necessarily in the long-term interests of preparedness. Beyond the unquantifiable human costs associated with hazards, figures from 2011 reveal that economic damages from natural disasters in the United States exceeded \$55 billion.² In 2012, there were many domestic disasters including Superstorm Sandy, lethal wildfires, regional droughts, domestic terrorism, and the spread of West Nile virus.³ While we must address immediate crises and apply the lessons learned from 9/11, Hurricane Katrina, the Haiti earthquake, and Deepwater Horizon oil spill, this study looks *Beyond the Storms* of pressing events to identify strategic opportunities that would make the nation better prepared and more secure through a new focus on systemic preparedness, response, and resilience.

This article documents the results of an exploratory study designed to examine the state of preparedness in the United States by drawing upon policy reviews, case studies, and expert interviews. The relevant body of literature and policies addressing preparedness and critical infrastructure protection is informed by academic, private sector, cross-governmental, and security imperatives with a focus on the post-9/11, post-Katrina threat environment of natural disasters, terrorism, cyber-attacks, and health pandemics. Against that backdrop, this article is focused on the following themes:

- The *current state of preparedness* based on policy directives to prevent, protect from, mitigate, respond to, and recover from disasters;
- Understanding the *complexity and interdependencies* of critical infrastructures and central role of global supply chains;
- The assertion of *resilience as a public good* enabled by collective action, interagency coordination, and public-private partnerships (PPPs);
- The ability of cross-governmental stakeholders to *implement policy* under the current whole-of-nation interagency constructs; and

¹ *National Security Strategy* (Washington, DC: The White House, 2010); Thad Allen, “The Future of Homeland Security: The Evolution of the Homeland Security Department’s Roles and Missions,” Testimony before the U.S. Senate Committee on Homeland Security and Government Affairs, *U.S. Senate*, July 22, 2012, available at: <http://www.hsgac.senate.gov/hearings/the-future-of-homeland-security-the-evolution-of-the-homeland-security-departments-roles-and-missions>.

² Committee on Increasing National Resilience to Hazards and Disasters, Committee on Science, Engineering, and Public Policy. *Disaster Resilience: A National Imperative*. Washington, D.C.: The National Academies Press, 2012. Print.

³ One NGO estimates there were 1,274 anti-government groups at the end of 2011, up from 131 groups four years ago.

- Potential *remedies to strengthen preparedness, response, and resilience* in support of all-hazards safety, security, economic, and environmental objectives.

More than Critical Infrastructure Protection

The initial focus of this study was on critical infrastructure protection (CIP), but ultimately extended to the broader concepts of preparedness and resilience, as the research pointed toward a broader strategic view. It is clear that disaster management planners, and leaders across public-private sectors, understand how to build and protect infrastructures within their areas of responsibility, but often lack awareness of the challenges facing adjacent geographic or infrastructure sectors. Therefore, there is a significant lack of resilience thinking, integrated planning, and collective action at the national, regional, state, and local level.

Empirical data revealed a fragmented planning and risk assessment process where agencies tend to focus narrowly on their areas of concern (ports, bridges, railways, tunnels, telecommunications, power, water, etc.), yet fail to recognize the complex interdependencies of the broader homeland security enterprise. Furthermore, when preparing budget requests or proposals for grant funding, submissions reflected this isolated approach that safeguarded their specific region or municipality at the expense of the collective good. Initial findings uncovered that while we live in an interconnected world of complex 21st century vulnerabilities, we often employ 20th century ways of thinking and planning for security – allocating resources for physical protection based on the most senior member on the congressional committee, best-written grant proposal, or a bias for “fixing things” to relieve the most immediate pain.

Current State of Preparedness

In the past century, catastrophic disasters have brought dramatic reminders that we need to better understand risk mitigation and how to improve critical infrastructure resilience. It recognizes that some 85 percent of all critical infrastructures, across sixteen independent sectors, are owned and operated locally or regionally by the private sector and often influenced by an uncoordinated mixture of investors, volunteers, non-profit organizations, labor unions, and utilities; and the federal government is often hard-pressed – or simply unable – to institute changes.⁴

It is increasingly clear that the nation needs a new resilience-based approach to critical infrastructure protection that can be integrated into the homeland security enterprise and builds greater trust across public and private stakeholders. Action plans are needed – not just government strategy documents – to implement preparedness policies and incentivize the private sector to support policymaking, equity investments, cost recovery, new insurance markets, and legislative changes, or the nation’s infrastructure will remain in the current state of disrepair.⁵ Researchers and global innovators emphasize the futility of popular security habits (with a

⁴ “Critical infrastructures” are systems and assets, whether physical or virtual, so vital to the nation that their incapacity or destruction would have a debilitating impact on national security, economic security, public health or safety, or any combination of those areas (USA Patriot Act of 2001, Section 1016e); Flynn, Stephen, *The Edge of Disaster – Rebuilding a Resilient Nation* (New York: Random House, 2007); National Infrastructure Advisory Council (NIAC), *Cross Sector Interdependencies and Risk Assessment Guidance*, January 13, 2004, available at: www.dhs.gov/xlibrary/assets/irawgreport.pdf.

⁵ Thad Allen, “The Future of Homeland Security.”

fixation on physical protection), and assert the need for new, more pragmatic resilient approaches because “the holy war against the boogeymen hasn’t worked and isn’t likely to anytime soon.”⁶

There is a clarion call for a shift in disaster preparedness that places a sharp focus on resiliency. The statistics predict a looming challenge that is not well understood by a population that expects critical infrastructures to automatically serve their needs. For example, approximately 75 percent of the nation’s gross domestic product (GDP) is fueled by metro communities while over 80 percent of the U.S. population is located in eleven mega-regions, where new approaches to resilience-thinking are needed most. The risk assessments and analytical frameworks which model the infrastructure resilience in an interconnected environment must be developed to better understand these complex urban communities, as underscored by the cascading regional impacts caused by disasters such as the October 2012 Superstorm Sandy. Now that federal funds are receding, there is a need for increased private sector participation and regional approaches to address the “wicked problems” being faced by preparedness planners. The 90,000 local, regional, and state flood maps maintained by the Federal Emergency Management Agency (FEMA) are incomplete or outdated as extreme weather conditions have revealed in recent years; and corresponding products – risk maps – for the regional all-hazards threat environment do not exist.⁷

A Nation at Risk

The United States is at a critical juncture where many infrastructures are aging or failing, and current efforts to address the challenge are insufficient. America invests barely 2 percent of its GDP in infrastructure renewal and maintenance, one of the lowest figures among the world’s industrialized nations. The following facts expose some of our demographic and infrastructure fault lines:

- Using input from engineers in every state, the American Society of Civil Engineers (ASCE) gave the national infrastructure an overall grade of D-plus, a score impacted by failing areas such as aviation, drinking-water-supply, roads, transit, and sewage treatment;
- 42 percent of the nation’s urban highways are congested, which costs our economy more than \$101 billion annually in lost time and fuel, while increasing harmful exhaust and pollution;
- 38 percent of the roads are in disrepair and the U.S. must invest \$225 billion per year over the next fifty years to maintain and enhance a decaying surface

⁶ Zolli, Andrew and Ann Marie Healy, *Resilience: Why Things Bounce Back* (New York: Free Press, 2012).

⁷ U.S. Department of Homeland Security (DHS), Office of the Inspector General (OIG). *Challenges in FEMA’s Flood Map Modernization Program*. Report No. OIG-05-44 (September 2005); U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*. Report No. GAO-10-296 (March 2010); Morton, John and Catherine Feinman, *DomPrep Action Plan: Building Resilient Regions for a Secure and Resilient Nation* (Severna Park: IMR Group, Inc., 2012); National Infrastructure Advisory Council (NIAC), *Regional Resilience Scoping Study*, March 23, 2012, available at: <http://www.dhs.gov/xlibrary/assets/niac/niac-regional-resilience-white-paper-032412.pdf>.

transportation system; we are currently spending less than 40 percent of this amount;

- The U.S. operates 361 major ports and delivers \$13 billion containers globally per year, supporting the world's largest trading commerce (\$645 billion), yet there is no executive agent assigned to manage or integrate this dynamic global supply chain and associated policies;
- The Army Corps of Engineers estimates that over 95 percent of overseas trade produced or consumed by the U.S. moves through our nation's commercial ports. Yet, our ports are in danger of losing their competitive advantage due to the slow and very complex process of critical dredging projects;
- By 2020, every major U.S. container port is projected to be handling at least double the volume it was designed to handle, and by 2040, this figure is projected to triple;
- Over the next twenty years across the nation, railroads are projected to need nearly \$200 billion in investments to accommodate increased freight traffic;
- Over 25 percent of the nation's bridges are considered structurally deficient;
- There are approximately 85,000 dams in the country, averaging over fifty years old, and 4,000 are considered structurally at risk; and
- There are 500 major urban public transit operators, 66,000 chemical plants, over 2,800 electric plants, 104 nuclear power plants, 1,600 municipal waste water facilities, over two million miles of pipelines, 87,000 food processing plants, and 5,000 public airports owned and operated independently; however, they are highly interdependent in their functional capabilities.⁸

The Issue of Our Day

This sampling of facts bespeaks a menacing challenge that must be addressed with a sense of urgency or infrastructure systems will continue to erode along with public safety and security. Many believe that this challenge – to dramatically transform how we secure and maintain our critical infrastructure through a posture of resilience – is the “issue of our day.” As the “Greatest Generation” confronted the threats from Germany and Japan in World War II, and proceeded to build the domestic infrastructure system that has been enjoyed for the past sixty years, the current generation also faces defining challenges. There is a need for a comparable resolve in facing today's serious challenges – including economic austerity, natural disasters, and global

⁸ U.S. Government Accountability Office (GAO), “Critical Infrastructure: Challenges Remain in Key Sectors,” Testimony before the Committee on Appropriations, Subcommittee on Homeland Security, *House of Representatives*. Report No. GAO-07-626T (March 2007); Gerencser, Mark, Van Lee Reginald, Fernando Napolitano and Christopher Kelly, *Megacommunities: How Leaders of Government, Business, and Non-Profits Can Tackle Today's Global Challenges Together* (New York: Palgrave Macmillan, 2008); Byram, Daniel (Ed), *Introduction to Homeland Security* (New York: Pearson Custom Publishing, 2009), 164-65; Thad Allen, “The Future of Homeland Security.”; *A New Economic Analysis of Infrastructure Investment: A Report Prepared by the Department of Treasury with the Council of Economic Advisors* (Washington, D.C.: U.S. Department of Treasury, March 23, 2012); Haya El Nasser, “American Cities to Millennials: Don't Leave,” *USA Today*, December 4, 2012, available at: <http://www.usatoday.com/story/news/nation/2012/12/03/american-cities-to-millennials-dont-leave-us/1744357/>; American Society of Civil Engineers (ASCE), *2013 Report Card for America's Infrastructure* (Reston: ASCE Publications, 2013).

security threats – to forge a culture of preparedness and invest wisely in critical infrastructure resilience.

Globalization and expanded markets have unwittingly introduced the potential for greater cascading hazards. Many of the freedoms that accompany technology and social networking advancements have in fact made us more vulnerable. This study reinforces observations made since the Y2K scare thirteen years ago, when spending by the U.S. government and commercial industry to predict and prevent adverse impacts on critical infrastructures exceeded \$100 billion. During this time period, the lessons of globalization and cyber security suggest that vulnerabilities from “system complexity” have expanded at a faster pace than our means of mitigating them. Further, interconnected infrastructure systems, while offering greater speed and efficiency, now present larger targets for potential exploitation by criminals and terrorists because these networked architectures are operated in an open society.⁹ The qualities of speed, access, and anonymity that make these robust systems so effective are the same features that make them more vulnerable to nefarious elements.

Threats to our physical and virtual security are complex, new, and growing. They demand a new approach to how we prepare for attacks and sustain our infrastructure, as well as how we mitigate, respond to, and recover from crises. Many of the threats we face *cannot* be deterred or countered simply because the provision of civil liberties and a free society are paramount. The idea that complete physical security is normal, or even achievable with enough Transportation Security Administration (TSA) agents and Customs and Border Protection (CBP) officers, is an illusion that is consuming our finite economic resources.¹⁰ Our focus must be fixed on building a new vision of 21st century resilience in the face of uncertain and complex risks.¹¹

Hope and Hubris

This new vision starts with a careful examination of cultural mindsets and deeply held attitudes toward emergency hazards. All disasters are personal, and the first priority in preparedness planning is an *individual* responsibility. According to FEMA guidelines, people should be self-sufficient for seventy-two hours after a disaster strikes if evacuating, and longer if sheltering-in-place.¹² That is where the breakdown often begins. Experts emphasize that America will never truly mitigate the harsh impact of disasters until the public takes personal ownership for the preparations necessary to respond to and recover from emergencies.¹³

⁹ Mussington, David, *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development* (Santa Monica: RAND, 2002).

¹⁰ The 9/11 hijackers spent less than \$1 million to attack the United States; while the cost to try to prevent similar future attacks (in police, airport security, and monitoring systems) costs Americans a million dollars an hour.

¹¹ Flynn, Stephen and Burke, Sean, *Critical Transportation Infrastructure and Societal Resilience* (Washington, DC: Center for National Policy, 2012).

¹² Insurance Institute for Business & Home Safety (IIBHS). *Know Your Plan – Prepare for a Disaster*, 2012, available at: <http://disastersafety.org/earthquake/disaster-planning-there%e2%80%99s-an-app-for-that/>.

¹³ U.S. Department of Homeland Security (DHS), *National Response Framework*, 2008, available at: <http://www.dhs.gov/xlibrary/assets/NRF.pdf>; U.S. Department of Homeland Security (DHS), *National Infrastructure Protection Plan*, 2009, available at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf; Federal Emergency Management Agency (FEMA), *A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action* (Washington, D.C.: FDOC-104-008-1, 2011).

The challenge of raising public awareness about preparation before a disaster strikes is manifested in an attitude: “It will not happen to me,” or “We will just deal with it at the time.” While clearly a dangerous reaction, as learned from hurricanes Katrina, Irene, and Sandy, it can also be linked to difficult economic times. A society struggling with poverty and unemployment is focused on financial survival and is therefore, less likely to spend essential money (or even discretionary funds) on insurance or redundant systems that don’t have an immediate return on investment (ROI) or help “to pay the bills.” Yet, research indicates there is a 4:1 ratio associated with preventive action supporting infrastructure; for every dollar spent now on resilience-building and disaster preparedness, one can avoid at least four-dollars in future losses. However, an investment in resilience is often considered an “invisible” payoff, because if built and maintained properly, infrastructure works as planned and life continues uninterrupted.¹⁴

In addition to an attitude of denial, many people simply refuse to take ownership for individual preparation because “It is the government’s responsibility, and FEMA will take care of us.” This attitude must be challenged through a combination of initiatives at the local, regional, state, and national levels.¹⁵ Because extreme weather, terrorist attacks, and health epidemics are inevitable, citizens should rely less upon outside assistance and depend more upon their personal resources, enabling communities to be better prepared for future disasters. Additionally, rather than creating a new “program” that would add another financial burden to already-struggling families and small-business communities, there should be incentives that can be applied to existing (family and small business) financial budgets to “reward” action taken to support resilience. Although federal funds are needed to implement some programs, many requirements can – and should – be accomplished through state-level programs.¹⁶

Moving beyond human factors to an all-domain context (land, maritime, air, space, and cyber), the next section will introduce a framework that draws upon the current pillars of national preparedness (prevent, protect, mitigate, respond, and recover), offering a continuum of options from infrastructure protection to functional continuity under a broad umbrella of resilience (Figure 1). This framework suggests a view of resilience that helps define the planning variables involved in national preparedness. There is an important distinction between “protection” – which focuses on the *threats*, and “continuity” – which focuses on *resuming operations* despite the consequences. In this framework, both objectives are enabled through the operating principles of *resilience*. And while prevention and protection may be the preferred options in

¹⁴ American Society of Civil Engineers (ASCE), *Guiding Principles for the Nation’s Critical Infrastructure* (Reston: ASCE Publications, 2009); Kerry, John, Frank Lautenberg and Kirsten Gillibrand, “Strengthening the Resiliency of Our Nation on the Ground (STRONG) Act (S-3691),” *Library of Congress*, available at: <http://beta.congress.gov/bill/112th-congress/senate-bill/3691>.

¹⁵ Kettl, Donald, *System under Stress: Homeland Security and American Politics*. (Washington, D.C.: CQ Press, 2004); U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection*, 2010; American Red Cross, *Web Users Increasingly Rely on Social Media to Seek Help in a Disaster*, August 9, 2010, available at: <http://www.redcross.org/portal/site/en/menuitem.94aae335470e233f6cf911df43181aa0/?vgnnextoid=6bb5a96d0a94a210VgnVCM10000089f0870aRCRD>; U.S. Department of Homeland Security (DHS), *National Response Framework*, 2008, available at: <http://www.dhs.gov/xlibrary/assets/NRF.pdf>; Morton and Feinman, *DomPrep Action Plan*, 2012.

¹⁶ U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection*, 2010.

many cases, they are not always possible. Therefore, an increased focus is needed on mitigation, response, and recovery.¹⁷

Figure 1: Resilience Framework

Understanding Resilience

Resilience, in a physical and structural sense, is considered “the ability to bounce or spring back into shape or position after being pressed or stretched.” However, the broader concept of resilience originated in the ecological and social sciences, where it is critical for survival and growth within complex systems. Research on these systems suggests that they perpetually evolve through an “adaptive cycle” of growth, crisis, transformation, and renewal. Resilience is not only the ability to recover from disasters and flex – instead of snapping – but is also the ability to *get stronger* as a result of adversity.¹⁸

The traditional view of physical security and infrastructure protection involves preparing for risks and dangers we do not know about, hardening facilities against a potential attack, and adding more redundancies and defensive layers; analogous to an individual saving money in case of a job-loss. However, resilience suggests a different type of preparedness where one would, in addition to saving money, learn new skills and establish a broader network to land a better job.¹⁹ In the case of critical infrastructure, rather than “fixing things” or adding more safeguards through the congressional appropriations and authorization process, we should systematically evaluate where and how we can make optimal investments to rebound from a disaster, and in some cases, pre-position recovery resources and have trained response teams on stand-by.

Among the various perspectives on resilience held by engineers and social scientists, the Multidisciplinary Center for Earthquake Engineering Research (MCEER) offers common actions to achieve resilience across all infrastructure sectors that are arguably inadequate for modern

¹⁷ John Moteff, “Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress,” *Congressional Research Service*, August 23, 2012, available at: <http://www.fas.org/sgp/crs/homesec/R42683.pdf>.

¹⁸ Gunderson, L.H., C.S. Holling and D. Ludwig, *Panarchy: Understanding Transformations in Human and Natural Systems* (Washington, D.C.: Island Press, 2002).

¹⁹ Cooper-Ramo, Joshua, *The Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us* (New York: Back Bay Books, 2009).

levels of complexity: robustness, redundancy, resourcefulness, and rapidity. These traditional measures signal the need for innovative thinking that goes beyond simply investing in more “guns, gates, guards, and locks” in order to protect physical structures. We must identify the capabilities needed to mitigate the impact of, and respond to, *inevitable* hazards. Oftentimes, it is nearly impossible to determine the risk of hazards because there is too much uncertainty to quantify the threats, vulnerabilities, or consequences. The variables in the equation can be so complex that this information is sometimes unknowable.²⁰

Therefore, the best return on investment – and source of confidence – across interdependent supply chains, infrastructure sectors, and interconnected systems is not a fortress-protection mentality, but an investment in “functional resilience” that imbues communities with a level of confident anticipation and personal preparation for inevitable disasters looming over the horizon. In a post-9/11, post-Sandy, post-H1N1 environment, we should no longer be surprised by disastrous interruptions to our otherwise normal lives, but should anticipate, and even expect, them. We should prepare with a resilient mindset even if it does not come naturally.

The Way Ahead—Functional Resilience

Functional resilience is a broad term used in building codes, environmental design, and civil engineering that involves making systems more durable and disaster-resistant through agile and adaptive approaches. Beyond extending the effective life of systems, functional resilience allows them to operate more efficiently, demanding fewer resources for repair and emergency response because flexibility is incorporated into the initial design.²¹ The comprehensive application of this concept to preparedness and critical infrastructure resilience, along with the necessary assessment tools, has yet to be realized. There is encouraging work underway that includes computational models, operations research, and human factors, but there is a need to operationalize functional resilience in a coordinated and systematic manner.

The principles of functional resilience complement existing public policies. The fundamental objective of national preparedness is to take a holistic approach, focusing on systemic investments that enable the enterprise to absorb the impact of a disaster event without losing the capacity to function. The supporting taxonomy, focused on large-scale optimization, must identify the functional capabilities of the national infrastructure system that are most important by geographic area, and help decide where to invest limited fiscal resources.²²

Building on this concept of functional resilience, how would one build a framework that is useful across local, state, and federal equities within the homeland? First, it must operate in parallel with traditional physical protection, because there will always be mission-essential locations that need to

²⁰ Bruneau, Michel, et al, “A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communications,” *Earthquakes Spectra* 19:4 (2003): 733-752; Cooper-Ramo, *The Age of the Unthinkable*, 2009.; Zolli and Healy, *Resilience: Why Things Bounce Back*, 2012).

²¹ Gunderson, L.H., C.S. Holling and S.S. Light, *Barriers and Bridges to the Renewal of Ecosystems and Institutions* (New York: Columbia University Press, 1995).

²² U.S. Department of Homeland Security (DHS), *National Strategy for Homeland Security* (Washington, D.C.: Department of Homeland Security, 2007); U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection*, 2010.; *Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience* (Washington, D.C.: The White House, 2013).

be hardened against and protected from disaster. Second, it requires a capabilities-based approach with standard assessment criteria to determine where functions are assessed and located on the continuum of preparedness (between protection and continuity). Which functions are essential such that there is no tolerance for degradation; which ones can withstand disruption and some period of recovery; and which fall somewhere in-between with a mixture of functional capabilities?²³ The criteria needed to make these judgments is developed by mapping the unique interdependencies of each geographic region, identifying the appropriate independent variables, and leveraging the tools of both qualitative and quantitative research.

The goal is to better understand the nature of risk based upon essential functional requirements rather than on uncertain physical threats. Therefore, working with researchers, owners/operators, and policymakers, we need to introduce an effective framework (Figure 1) that is adaptable and scalable to various geographic and infrastructure areas. Rather than a policy document that tries to fit all scenarios (which will be ignored by planners if not clearly relevant), guidance should take the form of a general framework that is scalable, recognizing that credible threat information is often unavailable. By introducing a framework or model that can be applied across the range of functions and capabilities as general guidance, state and local authorities can better implement critical infrastructure and key resource (CIKR) and disaster management requirements. The utility of this resource will be demonstrated by how well future decisions are made regarding maintenance and repair priorities, and strategic funding, in order to strengthen preparedness and sustain critical infrastructure resilience.²⁴

This framework will offer the ability to align local, state, regional, and federal resiliency priorities in an integrated fashion that supports the greater good rather than the individual pet-projects of political officials. For example, the Port of Los Angeles (POLA) moves more containers than any other maritime port in the country, providing intermodal access to 14 major freight hubs across the nation, and invests approximately \$1 million per day in capital improvements. And how should the POLA and local ports (with eighty-eight different municipalities) best invest their scarce resources at such a critical transportation hub in the country? The question should be answered against a measurable set of capabilities-based criteria designed to achieve functional resilience in the face of certain and uncertain risks.

Many Creative Ideas and Partners Available

The encouraging news is that the United States is not alone. There are international partners who face similar challenges and are willing to share information, and professional fora to draw upon academia, public-private partnerships, and the experience of commercial industry to improve preparedness. We can no longer afford—financially, technologically, or environmentally—to take a unilateral approach toward preparedness when facing a globalized system of interdependent supply chains and infrastructure sectors.²⁵

²³ Within the CIKR and resilience context, the analysis expands beyond simply physical or single-sector locations to include “function” – the purpose for which something is designed; a specified role, action, or capability.

²⁴ National Infrastructure Advisory Council (NIAC), *Cross Sector Interdependencies*, 2004.; National Research Council (NRC), *Building Community Disaster Resilience Through Private-Public Collaboration* (Washington, D.C.: National Academies Press, 2010); Morton and Feinman, *DomPrep Action Plan*, 13.

²⁵ National Infrastructure Advisory Council (NIAC), *Best Practices for Government to Enhance the Security of National Critical Infrastructures*, April 13, 2004. available at:

This study provides a new taxonomy that will help the nation and leaders committed to supporting resilience initiatives, understand how to: (1) make the case more clearly to policymakers and senior decision-makers, (2) leverage the capabilities of international partners, (3) incentivize investments from private equity sources, (4) start mapping functional interdependencies, and (5) build a capabilities-based model to advance the concept of resilience. Below are some exemplars that may help inform the efforts of preparedness planners in the public and private sectors:

- Military and interagency studies on unrestricted, irregular, and unconventional conflict provide a relevant body of literature and critical thinking because of the similarities to complex and asymmetric factors that are present within critical infrastructure resilience and all-hazards environments;
- Academic institutions and Homeland Security Centers of Excellence across the country are actively studying and testing many of the issues surrounding preparedness and critical infrastructure resilience, generating research-based models to help inform strategic and operational planning;
- After the attacks of 9/11, aviation transportation was grounded for three full days as a security precaution; and the maritime ports, with the exception of the Ports of Los Angeles and Long Beach (POLALB), California, were closed, disrupting vital commerce and trade. Actions by the POLALB provide an example for centers of intermodal activity and complex interdependencies during future incidents, where advanced planning communications among emergency management, law enforcement, port authority, regulators, labor unions, and congressional leaders allowed increased security and sustained port operations to occur simultaneously;
- Counterparts to Homeland Security and FEMA planners in the British Cabinet Office's Civil Contingencies Secretariat have successfully implemented "business continuity" strategies with the private sector by leveraging the relationships that small and medium-size enterprises already trust and rely upon: suppliers, customers, banks, insurance companies, professional organizations, and distributors;
- United Kingdom (UK) officials conduct an annual National Risk Assessment (since 2005), and publish an unclassified National Risk Register of Civil Emergencies to explain—in terms that are clear to the general public—what an emergency is and the types of risks (natural hazards and terrorist threats) that government planners are prepared for; and they offer on-line resources to summarize how members of the public should prepare;
- The Australian National Security Strategy reflects a *Beyond the Storms* approach, placing "ensure a safe and resilient population," and, "secure our assets, infrastructure, and institutions" as two of their four strategic national security objectives. One of the eight pillars to support these objectives is "strengthening resilience" across their society. Recognizing "it is not possible to eliminate all

http://www.dhs.gov/xlibrary/assets/niac/NIAC_BestPracticesSecurityInfrastructures_0404.pdf; U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*. Report No. GAO-10-296 (March 2010).

risks to national security,” they place a focus on public-private partnerships and building community cohesion in order to “respond and recover quickly” to restore essential services.²⁶

The Implementation Challenge—Public Private Partnerships

The key to implementation of any local, state, regional, or national level policies in support of critical infrastructure resilience, preparedness, or business continuity is *leveraging the utility of public-private partnerships*. While many of the strategies and policies that inform these public policy challenges originate from federal or state-level intergovernmental agencies most disaster management and emergency response activity occurs at the local level among private sector owners and operators. And since some 85 percent of critical infrastructures are managed by the private sector, the greatest advancements in community resilience will stem from the actions of private-sector stakeholders.

Strategic policies and national strategies assert the importance of expanding public-private partnerships (PPPs) and acknowledge the need to incentivize venture capitalists in supporting infrastructure improvements and disaster preparedness, but few details have emerged in academia, think-tanks, or public policies identifying *how* to incentivize these communities, infuse private sector investments, or significantly expand PPPs. Private industry is in the business of making money by seeking investments that will reduce risk, demand less manpower, and provide a reliable flow of revenue in the current fiscal climate. As the public sector seeks to remove barriers and incentivize the private sector to increase participation in joint ventures and partnerships, there will be a natural resistance to form PPPs within commercial industry because anything that could provide competitors with a market advantage is not something they will be interested in.

To help put this issue in context for both government planners and commercial industry, consider the economic impact of a port strike and the amount of revenue the private sector might lose. Estimates can vary widely, but experts claim that an eleven-day lockout at ports on the West Coast in 2002 cost the economy approximately \$1 billion per day. More recently, in December 2012, this situation reared its head in the POLALB, where a strike by union clerical workers resulted in the closing of ten terminals at the nation’s busiest port complex, costing the local economy billions of dollars over a two-week period—and forcing some ships to sail to other west coast ports to offload their cargo.²⁷ Not only will dockworkers refuse to cross picket lines established by union workers who are striking for a new contract, but private companies will not share information that would in any way weaken their market position with other ports. When preparedness or resiliency policy is developed, policymakers must look at both the national interests as well as local economic realities that drive industry decisions. For example, rerouting of shipping-container traffic from POLALB to another west coast port-of-entry may support

²⁶ Australian Government, Department of the Prime Minister and Cabinet, “Strong and Secure—A Strategy for Australia’s National Security,” *Australian National Security Strategy*, January 23, 2013, available at: <http://www.nationalsecurity.gov.au/>.

²⁷ Brad Plumer, “Could a Port Strike Really Cripple the U.S. Economy?” *The Washington Post*, December 27, 2012, available at: <http://www.washingtonpost.com/blogs/wonkblog/wp/2012/12/27/could-a-port-strike-really-cripple-the-u-s-economy/>.

national policy objectives and preparedness calculations, but it's not likely to be a model that the ports will support.²⁸

Figure 2: Port of Los Angeles²⁹

National Call to Action

The major findings from this study underscore areas that must be addressed by the nation – at the local, regional, state, and federal level – if we are to establish a culture of community resilience within our society:

- The analysis of critical infrastructure protection and key resources point to broader strategic imperatives of preparedness, response, and *functional resilience*;
- Awareness of America's *economic dependence* upon outdated critical infrastructure and fragile global supply chains is lacking across the general public;
- The intersection of interagency coordination and collective action offers a *systematic approach* and practical utility to advance national preparedness;
- There is a need for a *functional resilience framework* to implement existing policies, strengthen regional resilience, and imbue a culture of preparedness;
- Because of *extensive interdependencies* across all infrastructure sectors, there are potential cascading impacts that can occur where local incidents trigger national-level degradation in services; and
- *Further study is needed* to examine regional dependencies and interdependencies, operationalize public-private partnerships, and craft a whole-of-nation campaign for action.

²⁸ Michael Orosz, *Personal Interview and Email Communications* (Decision Systems Group, Computational Systems & Technology, Information Sciences Institute, Viterbi School of Engineering, University of Southern California, Marina del Rey, CA), July 9, 2012 and December 24, 2012.

²⁹ Madlyinlovewithlife (Flickr username). *Cargo Cranes, Port of Los Angeles, CA*. February 7, 2009, available at: <http://www.flickr.com/photos/madlyinlovewithlife/6044091310/>.

Drawing from these strategic findings, a team of researchers, analysts, and planners are taking steps to address some of the major challenges outlined in this article. These efforts will serve as a catalyst among public and private-sector leaders to nationally expand awareness of preparedness and operationalize *critical infrastructure resilience*:

- (1) Systematic *risk-mapping* of infrastructure dependencies and interdependencies in specific geographic areas to understand *what* the essential ligaments of preparedness and resilience are for complex intermodal systems. By employing scenario-based analyses, one can understand the potential impact of a disaster and conduct a nodal analysis to understand connectedness between and among critical infrastructures. The outcome of this effort will be a “risk map” that identifies intermodal variables, single-points-of-failure, and supporting interdependencies;
- (2) Developing a *functional resilience framework*, using an integrated approach which helps planners identify *how* to proceed, and prioritize capability gaps in preparedness and resilience. Drawing from both qualitative and quantitative assessment criteria, as well as the outputs of the risk mapping effort, business rules and mitigating actions will be identified that allow emergency planners to focus on the most important functional areas. The outcome of this effort will be a conceptual methodology that can be generalized or adapted to other communities in scalable and flexible manner. The graphic representation of the framework will serve as a point of clarity to planners and practitioners who must begin to understand this approach as it applies to critical infrastructure resilience. It will also serve as key input to subsequent planning to implement unique actionable items for that geographic location; and
- (3) Formulating a *strategic action plan* to operationalize the outcomes from the first two phases, providing planners with leading indicators *where and when* events must be executed. During this phase policymakers must forge a consensus among private- and public-sector leaders regarding discrete projects, priorities, and implementation efforts. The outcome of this phase will be a roadmap that synchronizes the efforts necessary to achieve increased resilience, and may require new developments in governance, concepts of operations, and technology.

Conclusion

This article highlights the need for action in promoting resilience at local, state, regional, and national levels, which can be accomplished through awareness, planning, resource allocation and strong leadership.³⁰ In order to operationalize these themes, this study asserts the importance of collective action in addressing national-level preparedness through expanded interagency coordination and increased private sector participation. Building upon functional continuity, preparedness, and disaster management principles (Figure 1), there is a need to better understand resilience as an organizing principle to address national preparedness and CIKR imperatives. It is clear further research is needed to generate new data and models for understanding highly

³⁰ T. O’Rourke, “Critical Infrastructure, Interdependencies, and Resilience,” *National Academy of Engineering (NAE)* 37:1 (Spring 2007)

complex and uncertain environments. A systematic mapping of local, regional, state, and national capabilities-based requirements, based on a “functional” decomposition of all infrastructure dependencies and interdependencies is needed. As this study highlights, such research should be a high federal priority and be pursued aggressively with an all-hazards, intergovernmental, holistic approach to advance national preparedness and resilience objectives.

The findings of this study align with other major policies and initiatives, including Presidential Policy Directive 8 (PPD-8), Presidential Policy Directive 21 (PPD-21), the report, “Improved Disaster Resilience is Imperative to U.S.”, and the STRONG Act legislation.³¹ Both have emerged since August 2012, and represent a unique opportunity to build a “resiliency consensus” among public and private-sector planners. While these documents contain many strong recommendations, they *will not make a difference* when the next disaster impacts critical infrastructure systems unless leaders agree to collectively join with cross-government interagency, private sector, and academic actors to form a coalition of like-minded innovators. Disaster management planners must be willing to move *Beyond the Storms* of the immediate budget crisis and pressure to react to the most recent disaster, and team with others to resource, implement, operationalize, and measure this homeland security imperative. However, it will require extraordinary resolve and leadership to forge a consensus among a disparate group of local, regional, state, and national leaders to bridge the current divide between individual rhetoric and collective action.

³¹ *Presidential Policy Directive 8 (PPD-8) – National Preparedness*, (Washington, D.C.: The White House, 2011).; *Presidential Policy Directive 21 (PPD-21)*, White House, 2013.; National Academies, *Disaster Resilience*, 2012.; Kerry, Lautenberg and Gillibrand, “Strengthening the Resiliency of Our Nation on the Ground (STRONG).”