Operationalizing Critical Infrastructure Resilience

Dane S. Egli, Brian H. Donohue, Richard L. Waddell, John M. Contestabile, and Jonathon B. Cosgrove

ABSTRACT

Making the nation's infrastructure more resilient is crucial to protecting America from disasters and attacks; it is also vital to preserving America's economic strength and global influence. Toward that end, this article describes a practical framework for implementing resilience at all levels of government and the private sector. The article establishes the need to transition as a nation from critical infrastructure protection to a critical infrastructure resilience posture. It also emphasizes the necessity of community resilience informed by local and regional planners as well as public–private partnerships. To assist mayors, business owners, and national-level policy makers—who are all urgently preparing for future disasters—this article provides an organizing framework to mitigate hazards and improve preparedness through resilience.

THE NEED FOR RESILIENCE

A Nation at Risk

There is no safe harbor from the impact of catastrophic events such as disasters caused by extreme weather, earthquakes, and terrorism, or from the less visible effects of disruptive events such as those caused by pandemics, financial disturbances, and cyberattacks. These events have direct and 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. Our approach should leverage collective action principles to systematically strengthen preparedness, response, and resilience.

Recent disasters have had increasingly severe consequences. The policies associated with responding to these events continue to be reactionary. Despite its obvious utility, preparedness has not received the requisite attention to enable communities to potentially mitigate the impact of disasters before they occur. With an eye to the future, we must focus attention on enhancing our infrastructure's ability to withstand the various stressors that affect its functions. Beyond the unquantifiable human costs associated with hazards, National Oceanic and Atmospheric Administration figures from 2017 reveal that economic damages from weather-related

Note: This article draws heavily, and in many cases verbatim, from Egli, D., et al., *Facing the Storms: Operationalizing Preparedness and Critical Infrastructure Resilience*, APL, Laurel, MD (Sept 2013).

disasters exceeded $306 billion in the United States. These events included eight severe storms, three tropical cyclones, two flooding events, one wildfire event, one drought, and one severe freeze. While we must continue to improve our response to immediate crises and to apply the lessons learned from past disasters, we also need to look beyond those events to identify strategic opportunities that would make the nation better prepared and more secure through a new focus on systemic preparedness in terms of resilience.

Resilience is "the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies."[1] It is an active, collective, pervasive virtue that enables a society to withstand certain disruptions and learn in the process. Resilience requires innovating beyond our current culture and placing a new emphasis on mitigating, responding to, and recovering from disasters. It demands robustness, redundancy, rapidity, resourcefulness, and agility. More specifically, functional resilience seeks to absorb the impact of a disaster while still preserving the ability to perform essential functions—recognizing that most systems will withstand some level of degradation in the face of modern risks and must accept a period of incremental restoration.

Current State of Preparedness

Although adverse events affect individuals as well as infrastructure, raising public awareness about individual preparation before a disaster strikes remains a challenge. The attitude that "it will not happen to me" is common. Members of a society struggling with poverty, unemployment, or simply getting through the day are focused on financial survival and consumed by other distractions. Allocating money and time to procure insurance or redundant systems that do not have an immediate return on investment is not likely to be a priority for many.

However, with public buy-in, policy is more likely to change. Resources that have been typically dedicated to traditional response might be more effectively used in seeking greater resilience. Research indicates there is a 1:4 ratio associated with preventive action supporting infrastructure: for every dollar spent now on resilience building and disaster preparedness, one can avoid at least $4 in future losses.[2,3] However, investment in resilience is not readily seen or noticed, because if infrastructure is built and maintained properly, it essentially works as planned and life continues uninterrupted.

On the national level, reasons for choosing to deal with the immediate impact of an adverse event rather than the causes of the event itself may have roots in political, religious, or socioeconomic leanings or educational opportunities. The public often criticizes federal, state, and local governments' disaster response, expressing their opinions through various forms of media. Yet it is precisely these governmental bodies that are essential to responding to large-scale adverse events. Although individuals ultimately have to strive for their own well-being, it is the helping hand of the larger organizations supporting communities in need that might determine individuals' survival in the end. Nevertheless, public views do not always reflect the important role those organizations play. Some people believe that at least some of these organizations are for the most part wasteful. That "they also serve who only stand and wait" (Milton, "On His Blindness") may not be the overwhelming view taken by the public. So, if some portion of the public believes that investment in disaster response has minimal value, despite obvious and ubiquitous examples where responders' efforts have been critical to saving lives, it may be difficult to garner support for investment in resilience projects that the public cannot easily discern.

Still, bad times will come. Mitigating the impact of those bad times comes at a cost, whether more is invested in response or in making our systems and their components more resilient. We need a combination of initiatives at the local, regional, state, and national levels geared toward response and recovery to contend with these adverse events, but investment in the resilience aspects may prove the wiser investment. We should create incentives that can be applied to existing financial budgets to fund action supporting resilience. Although federal funds are needed to implement some programs, much could be accomplished through state-level or private-sector programs. We must develop the risk assessments and analytical frameworks that model infrastructure resilience in an interconnected environment to better understand the complex urban communities that make up our modern society. We need increased private-sector participation and regional approaches to address the hard problems preparedness planners face.

UNDERSTANDING RESILIENCE

Resilience, in a physical and structural sense, relates to 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. These systems 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 snap but also the ability to *get stronger* as a result of adversity. If we plan wisely, we have the chance to rebuild our systems so that they have greater functionality and efficiency.

The traditional view of physical security and infrastructure protection involves preparing for risks and dangers we do not know about, hardening facilities against potential attacks, 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. 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 that would allow us to rebound from a disaster and in some cases improve on system function.

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 their effective lives, functional resilience allows systems to operate more efficiently, demanding fewer resources for repair and emergency response because flexibility is incorporated into the initial design. Application of this concept to preparedness and critical infrastructure resilience, along with the necessary assessment tools, has yet to be realized. Encouraging work is under way 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 stressing 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 leaders decide where to invest limited fiscal resources.

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 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 so critical that there is no tolerance for degradation? Which ones can withstand disruption and some period of recovery? Which fall somewhere in between with a mixture of functional capabilities? (Within the critical infrastructure and key resources/resilience context, the analysis expands beyond simply physical or single-sector locations to include "function"—the purpose for which something is designed, such as a specified role, action, or capability.) The criteria needed to make these judgments must be 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 best return on investment and source of public confidence, across interdependent supply chains, infrastructure sectors, and interconnected systems, is provided not by a fortress-protection mentality, but rather by an investment in functional resilience that imbues communities with a level of confident anticipation and personal preparation for inevitable disasters looming on the horizon. We should no longer be surprised by disastrous interruptions to our otherwise normal lives; we should anticipate and even expect them. We should prepare with a resilient mind-set even if it does not come naturally.

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 the majority 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 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 public–private partnerships. Private industry is in the business of making money by seeking investments that will reduce risk, demand fewer personnel, 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 the formation of public–private partnerships within commercial industry because of the nature of market competition. When preparedness or resilience policy is developed, policy makers must look at both the national interests and the local economic realities that drive industry decisions.

To take one prominent example, Michael Bloomberg, former mayor of New York City, recognized the reality of extreme weather in future disasters and its impact on the local as well as the national economies. Bloomberg proposed investing $20 billion in what was called "managing the unavoidable."[4] The plan, which sought to make New York City resilient to future storms and disasters, proposed everything from new floodwalls to upgrading critical power and telecommunications infrastructures. The proposal is premised on the belief that Sandy-like storms will become more frequent in the future as the climate changes. The options, in Bloomberg's words, are to "do nothing and expose ourselves to an increasing frequency of Sandy-like storms that do more and more damage" or to "make the investments necessary to build a stronger, more resilient New York—investments that will pay for themselves many times over in the years to come."[5] In other words, resilience, not further emphasis on elusive prevention and physical protection programs—such as guns, gates, guards, and locks—is what is required to protect cities, populations, infrastructures, and commerce in the future.

The Economics of Resilience

By creating a more connected world, globalization has made new business efficiencies possible. Businesses have more supply-chain partners than ever before, allowing for greater specialization. Outsourcing leverages the benefits of comparative advantage. Purchasing from a single source reduces costs. And just-in-time delivery is reducing inventory and excess capacity. But these advances concurrently create a global system with little room for error and in which a local disruption can adversely affect the entire supply chain. This connectedness multiplies the consequences of high-impact but low-probability "black swan" events. And the costs are high.

A groundbreaking 2005 study by Kevin Hendricks and Vinod Singhal analyzed the effects of 827 disruption events.[6] The study found that over the course of 3 years, the average disruption reduced stock returns by an incredible 40%. The result was negative regardless of a disaster's cause. Infrequent and unlikely disruptions can, in a moment, destroy value created over a long period of time. Efficiency has inherent risk.

Supply-chain disruptions are common. Seventy-three percent of the respondents to the Business Continuity Institute's 2012 annual supply chain resilience survey had experienced at least one supply-chain disruption. Of these, nearly 40% occurred below the immediate tier-one supplier, underscoring the interconnectedness and complexity of modern business practices. Information technology and telecommunications outages were the top sources of disruption, with severe weather a close second. The primary consequences of disruptions reported by businesses are loss of productivity, increased cost of work, impaired service outcome, loss of revenue, and customer complaints.[7]

Therefore, supply-chain efficiency is not the whole story. Just as important is supply-chain *resilience*: the ability to withstand a crisis, absorb damage, recover quickly, and adapt to disruptive events. Resilience requires long-term planning and investment in redundancy, interoperability, and agility. Disruptions often cannot be predicted or controlled, but their negative effects are incontrovertible. As Hendricks and Singhal conclude, "Investments in increasing reliability and responsiveness of supply chains could be viewed as buying insurance against the economic loss from disruptions."[6]

In addition to mitigating the negative effects of supply-chain disruptions, resilience helps prepare businesses for economic downturns. According to Morgan Swink, the Eunice and James L. West Chair and Professor of Supply Chain Management at the Neeley School of Business, "A firm's ability to weather economic downturns, deal with volatility and manage costs under shrinking demands depends in large part on the resilience of its supply chains."[8] According to research he conducted with Nancy Nix, companies with supply-chain flexibility and adaptability are better able to reduce expenses during a downturn, allowing them to outperform competitors and achieve a substantially higher return on assets and equity.

Resilience is disaster agnostic, meaning it equally mitigates damage caused by earthquakes, terrorists, and economic downturns. And though it may be difficult to quantify generally, after every disaster businesses that prepared ahead of time come out on top.[9] For example, after the 2011 earthquake and tsunami in Japan, a semiconductor manufacturer that had developed a strategy to shift production to unaffected manufacturing plants in response to an earthquake 3 years earlier was able to restore full production more quickly than its competitors.[10] Maintaining critical operations in the face of disaster events confers a competitive advantage.

Far from being solely focused on economics, an approach that continues operations (maintaining the bottom line) and heightens security (protecting citizens) is likely the best response to a terrorist attack. The ultimate objective of America's enemies is not just a traumatizing attack on the population but also a punishing disruption of our economy. For example, al-Qaeda in the Arabian Peninsula (AQAP) claimed that the ignominious Christmas Day 2009 "underwear" bombing attempt was a success, even though the bomber was caught and stopped, because of the effect it had on air travel. AQAP said that the attempted attack was part of "Operation Hemorrhage," an effort to instigate fear and cause economic damage.[11] By this standard, 9/11—which caused rippling economic damage and inspired an enormous domestic and international reaction—was far more successful from the perspective of the terrorists than the 7/7 London Bombings, after which the British

public quickly returned to work.[11] The initial disaster is the terror attack, but a subsequent crisis occurs if we are unprepared and self-impose further stresses on the economy. Therefore, resilience capabilities can lessen the negative economic impact of future terrorist attacks and—at the same time—reduce the incentive to carry them out. Hence, good business practices and homeland security are enabled by resilience.

Investing in resilience is becoming a basic business practice. In addition to mitigating disaster-related damage, investment in resilience—by introducing new flexibility—can increase productivity, revenue, reputation, and shareholder value.[12] Investing in resilience before disaster strikes is the smart choice for companies and governments alike: such preparation helps to preserve critical capabilities and to restore functions quickly while denying terrorists their objectives and preserving economic prosperity.

THE RESILIENCE IMPLEMENTATION PROCESS

The resilience implementation process (RIP) is a general methodology that can be used in the public or the private sector at the local, state, and national levels to operationalize resilience and to help forge a consensus within the disaster management community. The process provides a prioritized action plan based on input from risk mapping and a functional resilience framework. The RIP has three parts (Fig. 1).

1. **Risk map.** This is a visualization of the current infrastructure condition at a particular geographic location. It depicts physical and virtual relationships in order to provide understanding of the level of connectedness across essential functions. Put simply, what is most important? What are the anticipated risks? What are the dependencies and interdependencies?

2. **Functional resilience framework.** The framework uses the risk map in an event-based analysis, examining capabilities during an incident based on the criticality of the functions they support. In other words, within a particular disaster scenario, what functions are critical? How capable and adaptive are these functions? What are the optimum gaps to close given the limited resources available?

3. **Action plan.** Leveraging the findings of the risk map and the analysis of the functional resilience framework, the action plan provides planners with indicators of where and when events must be executed. How do we implement what was found? How do we increase capability and decrease risk through a resilience-based approach to preparedness?

The RIP is designed to support preparedness-related decision-making for any system at any location. It uses a consequence-based approach that is concerned with the stressors that disrupt an organization's functions. This distinction helps identify and analyze cascading effects

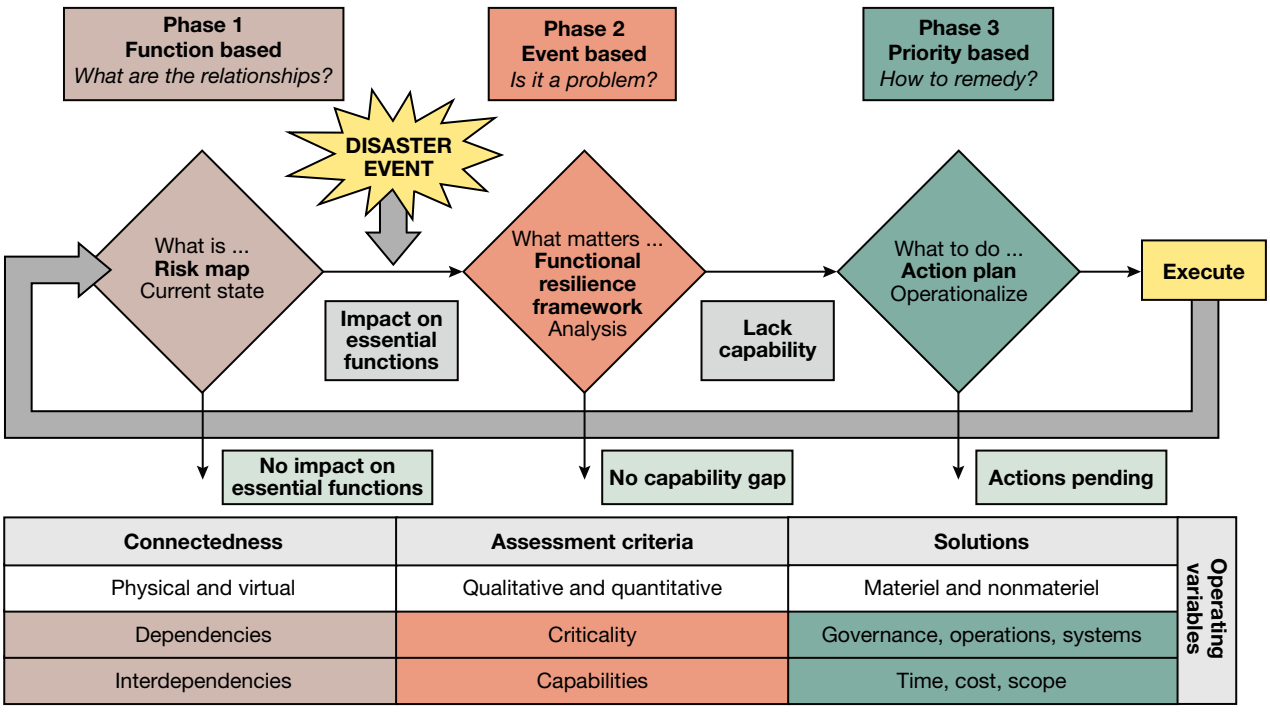

Figure 1. The resilience implementation process (RIP). (Reproduced from Egli, D., et al., *Facing the Storms: Operationalizing Preparedness and Critical Infrastructure Resilience*, APL, Laurel, MD, Sept 2013.)

in the aftermath of an event, informing the organization of potential vulnerabilities and single points of failure before they occur.

This framework offers planners, policy makers, and researchers a new approach to preparedness with a theoretical foundation of collective action and a practical implementation model to apply functional resilience. Five themes have shaped our approach and influenced the practical framework for evaluating resilience.

First, all disasters are local. Resilience matters most at the community level. Communities know what is important to them and must figure prominently in development of standards and risk maps.

Second, America needs a national framework for conception of resilience. Globalization makes us all interconnected. What one community does well—or poorly—often affects others in a cascading and disparate manner.

Third, resilience is a public good. Critical infrastructure is something Americans expect will function properly and be available for their use. It enables the basic functions of our society—power, transportation, communications, commerce, security, and independent living. Our critical infrastructure is the *sine qua non* of our way of life.

Fourth, only a combination of public and private actors can implement resilience. Some 85% of all infrastructures—across 16 independent sectors—are privately owned. Collective behavior among these parties is more likely if there are clear procedural or economic benefits. Accordingly, for resilience to succeed, incentives will need to be introduced and public–private partnerships formed.

Finally, the solution needs to meet the standard of common sense. A practical and efficient framework allows for easy understanding and implementation. The conceptual framework is designed with local-, regional-, and state-level planners in mind. It offers organizing principles that private-sector owners and operators can apply in catalyzing critical infrastructure resilience where it must start—at the grass roots of our communities.

A FUTURE VISION

"Of all the countries in the world," Alexis de Tocqueville contended in his 1833 *Democracy in America*, "America has taken greatest advantage of association and has applied this powerful means of action to the greatest variety of objectives." Contrasting America with other counties, Tocqueville admired the way Americans used voluntary associations to creatively and freely solve problems. Americans, he wrote, "associate for the goals of public security, of commerce and industry, of morality and religion. There is nothing the human will despairs of attaining by the free action of the collective power of individuals."[13] In a globalized economy with interconnected systems, only this spirit of innovation, this sense of personal responsibility, and this vision for collective action can effectively make American critical infrastructure more resilient.

Resilience is not a problem that can simply be handed to the government or studied by policy makers. It is a vexing challenge that crosses the boundaries of federal, state, regional, and local communities and transcends public-sector capabilities. Only a whole-of-nation public–private approach can offer an enduring solution. Furthermore, it is not enough to compile lessons learned from recent disasters: lessons *learned* are really lessons *observed* until they are operationalized. Functional resilience requires that we systematically distill the major lessons of these events *and* formulate a framework for action that can be implemented at the local, regional, state, and national levels.

Recognizing the major challenges of our era—eroding infrastructure, the growing interconnectedness of a globalized 21st century, and the emerging threats of climate change, natural disasters, and terrorism—in this article, we describe a holistic and generalizable framework to *prepare for* and *face* the storms of the future. There is a broad consensus that resilience *does* work and ought to be pursued as a matter of policy. The RIP is a starting point for all stakeholders to systematically prepare for the future by examining infrastructure, discovering complex interdependencies, defining functional resilience, and formulating action plans. The cumulative purpose of this effort is to mitigate the adverse impact of future disasters.

By increasing the flexibility and adaptability of American infrastructure, resilience makes the nation more secure from hostile actors, cyberattacks, and Mother Nature. By focusing on long-term mitigation and by rebuilding failing infrastructure, resilience also makes America more economically competitive because it facilitates the public goods that critical infrastructures provide. Like President Eisenhower's vision for the public highway system, resilience is both a national security objective and an economic imperative. While the benefits of resilience are unquestionable, it will still take a significant effort to integrate such thinking into our public–private communities and homeland security enterprise. Such an initiative is necessary to prepare the communities of America to face the coming storms.

REFERENCES

Note: This article draws heavily, and in many cases verbatim, from Egli, D., et al., *Facing the Storms: Operationalizing Preparedness and Critical Infrastructure Resilience*, APL, Laurel, MD (Sept 2013).

[1]Obama, B. H., *Presidential Policy Directive/PPD-8: National Preparedness*, The White House, Washington, DC (2011).

[2]Multihazard Mitigation Council, *Natural Hazard Mitigation Saves: An Independent Study to Assess the Future Savings from Mitigation Activities*, Vol. 1., http://www.floods.org/PDF/MMC_Volume1_FindingsConclusionsRecommendations.pdf (2005).

[3]Godschalk, D., Rose, A., Mittler, E., Porter, K., and Taylor West, C., "Estimating the Value of Foresight: Aggregate Analysis of Natural Hazard Mitigation Benefits and Costs," *J. Environ. Plan. Manage.* **52**(6), 739–756 (2009).
[4]Borenstein, S., "Climate Talks Shifts from Curbing CO2 to Adapting," Associated Press (15 June 2013).
[5]Russ, H., "New York Lays Out $20 Billion Plan to Adapt to Climate Change," *Reuters*, http://www.reuters.com/article/2013/06/11/us-climate-newyork-plan-idUSBRE95A10120130611 (11 June 2013).
[6]Hendricks, K. B., and Singhal, V., "An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm," *Prod. Oper. Manage.* **14**(1), 35–52 (2005).
[7]Business Continuity Institute, *4th Annual Survey: Supply Chain Resilience 2012*, https://www.zurich.com/_/media/dbe/corporate/docs/whitepapers/supply-chain-resilience-2012.pdf?la=en&hash=05476687F7FC361D0B423D1A887529E0E0E39E7C (2012).
[8]Neeley School of Business at TCU, *Weathering the Storm: How to Achieve Strategic Resilience Through Supply Chain Excellence*, http://www.neeley.tcu.edu/News_and_Events/Press_Releases/Weathering_the_Storm__How_to_Achieve_Strategic_Resilience_Through_Supply_Chain_Excellence.aspx (15 June 2012).
[9]Agrawal, M., and Church, C., *Resilience Return on Investment – An Impossible Argument?* Analytic Service, Inc., http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.642.3416&rep=rep1&type=pdf (2012).
[10]Marchese, K., Paramasivam, S., and Held, M., "Bouncing Back: Supply Chain Risk Management Lessons from Post-Tsunami Japan," *IndustryWeek*, http://www.industryweek.com/global-economy/bouncing-back-supply-chain-risk-management-lessons-post-tsunami-japan (9 Mar 2012).
[11]Stewart, S., "Keeping Terrorism in Perspective," Stratfor, http://www.stratfor.com/weekly/keeping-terrorism-perspective (22 Mar 2012).
[12]U.S. Resilience Project, *Business Case for Supply Chain Security and Resilience*, https://www.coursehero.com/file/10007656/USRP-Resources-Chapter-6-030112/ (1 Mar 2012).
[13]Alexis de Tocqueville, *Democracy in America*, J. T. Schleifer (trans.), Liberty Fund, Indianapolis, Part LI, Chap. 4 (2010).

Dane S. Egli, Strategic Consultant and Senior Advisor on National Security and Critical Infrastructure Resilience

Dane Egli has served as a program manager for the Department of Energy, National Nuclear Security Administration at Los Alamos National Laboratory; as national security advisor for APL, specializing in counterterrorism, homeland security, critical infrastructure, resilience, cyber, and maritime security; on the White House National Security Council staff as a director for counterterrorism and global counter-narcotics; and as senior advisor to the president on hostage rescue policy. He also chaired the interagency hostage working group. He is the founder and president of Cardinal Headings, LLC, focused on development of innovative technologies to support national security. He was president of Hyperloop Advanced Research Partnership (HARP), exploring the next generation of transportation infrastructure. He has a Ph.D. in public policy from the University of Colorado Denver, an M.S. in national security studies from the National War College, an M.A. in human resources management from George Washington University, and a B.S. in civil engineering from the U.S. Coast Guard Academy. His e-mail address is dane.egli@nnsa.doe.gov.

Brian H. Donohue, Force Projection Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Brian Donohue serves as APL's business continuity program manager while also focused on various efforts involving maritime logistics, high-valued asset security, maritime domain awareness, system resilience analysis, autonomy, sensor testing/development, and augmented reality. He has a background in modeling and simulation (M&S), remote sensing, image processing/analysis, geospatial technologies, and navigation, for application to planning, infrastructure development, research, and training, with particular application to the marine environment. Prior to joining APL, Donohue had maritime-related research and development experience that includes emphasis on technical analysis, design, software development, and system implementation as applied to M&S-relevant applications. He also has extensive maritime industry experience, both shoreside and at sea as a licensed officer in the U.S. Merchant Marine (license current), which includes stints in the offshore oilfield industry, intermodal operations, directing simulator-based studies, and sailing on various vessels involved in international trade. He completed coursework for a doctorate in applied ocean science at the University of Delaware. He has an M.S. in imaging science and engineering from New York University Polytechnic Institute and a B.S. in nautical science from the U.S. Merchant Marine Academy. His e-mail address is brian.donohue@jhuapl.edu.

Richard L. Waddell, Asymmetric Operations Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Richard Waddell is a program manager and systems architect in APL's Asymmetric Operations Sector. He has extensive experience developing and managing technology solutions for government sponsors in space robotics, transportation safety, homeland protection, and criminal justice. Current assignments focus on program management for criminal justice technology research, testing and evaluation, and homeland protection. Waddell oversees a portfolio of projects that typically start with analysis of the technology needs of state and local first responders and emergency managers in their operational environments and culminate in bottom-up solutions that meet users' needs and generalize to the broader public safety community. He has a B.A. in mathematics from Oakland University and an M.S. in applied mathematics also from Oakland University. His e-mail address is richard.waddell@jhuapl.edu.

John M. Contestabile, Asymmetric Operations Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

John M. Contestabile is a program manager for emergency response systems in APL's Asymmetric Operations Sector. He has been with APL for 10 years, leading a program focused on public safety/emergency responders at the local, state, and federal levels. He presently does work for the Department of Homeland Secu-

rity Science and Technology Directorate and the Cyber and Infrastructure Security Administration, FirstNet, and the National Institute of Science and Technology. He joined APL after a career at the Maryland State Department of Transportation where he retired as assistant secretary. There, he had responsibility for homeland security, emergency management, and transit rail safety and security. He participates in a number of national organizations, including as chair of the Resilience Section of the National Academies Transportation Research Board and chair of the Video Technology Advisory Group of the National Public Safety Telecommunications Council. He formerly served an appointment to the District of Columbia Homeland Security Commission and presently serves as an alternate member representing Maryland on the Washington Metrorail Safety Commission. He has a bachelor's degree in engineering from Worcester Polytechnic Institute and a master of business administration from the University of Baltimore. His e-mail address is john.contestabile@jhuapl.edu.

Jonathon B. Cosgrove, National Security Analysis Department, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Jonathon Cosgrove is an analyst in APL's National Security Analysis Department. Throughout his more than 6 years at APL, he has led and contributed to numerous studies tackling national security, strategy, policy, and organizational issues, with a special focus on adversary strategies as well as irregular and asymmetric warfare, for numerous sponsors. He holds an M.A. in statecraft and national security affairs from the Institute of World Politics and a B.A. in political science from Geneva College. His e-mail address is jonathon.cosgrove@jhuapl.edu.