SECURITY & CRITICAL INFRASTRUCTURE PROTECTION

Brittle Infrastructure, Community Resilience, and National Security

STEPHEN FLYNN AND SEAN BURKE

Flynn is President, Center for National Policy, Washington, D.C., and Chair of the Steering Committee for the Community Resilience System Initiative of the Community and Regional Resilience Institute, Oak Ridge, Tennessee. Burke is Vice President and Senior Fellow at the Center for National Policy.

Resilience in response to chronic and catastrophic risks is the key to assuring security, safety, and prosperity in the 21st century. Turbulence fueled by unconventional conflict, likely changes in climate, and the sheer complexity and interdependencies of modern systems and networks present ongoing challenges for years to come. This places a premium on assuring that individuals, communities, and critical infrastructure have the capacity to withstand, respond, recover rapidly, and adapt to man-made and natural disturbances.

PHOTOS: GARY COPPAGE, U.S. AIR FORCE; BRANDAN W. SCHULZE, U.S. NAVY

On Sept. 11, 2001, the Pentagon was struck by a hijacked commercial airliner and a section of the building was destroyed (*right*); the section was later rebuilt (*above*). The ability of infrastructure to absorb catastrophe is important to community security.

A lack of resilience entails a competitive disadvantage, because individuals and investors will gravitate away from localities and companies that cannot provide a continuity of essential services and operations. Resilience also serves as a deterrent to man-made threats—adversaries or terrorists who target resilient societies or systems find little disruptive return for their effort.

Civic Spirit

To obtain the benefits of resilience—and to counter the direct and indirect risks associated with fragile communities and systems—Americans must develop policies and incentives to encourage community initiatives at the local level, as well as within and across networks and infrastructure sectors regionally and nationally. Safety and security efforts that aim to eliminate risks reach a point of diminishing returns; often the more prudent and realistic investment is to manage risks by building the skills and capabilities to

- Maintain continuity of function during and after chronic disturbances,
- Develop the means for the graceful degradation of function under severe stress, and

◆ Sustain the ability to recover quickly to a desired level of function when extreme events overwhelm mitigation measures.

An emphasis on resilience provides a compelling rationale for cooperation and collaboration between the public and private sectors. At the community level, resilience requires a strong civic spirit—neighbors working with neighbors. Users, designers, operators, managers, and regulators have a shared interest in infrastructure resilience, and each has an important role in assuring the continuity of operations for essential systems and networks. Engaging and integrating the multiplicity of parties in a common effort to build a more resilient nation should be a priority.

When terrorists or disasters strike, the number of professionals in the right place at the right time is never sufficient. Intelligence and technologies are fallible, and forces of nature cannot be deterred. In detecting and intercepting terrorist activities or dealing with a catastrophic natural event, the first preventers and responders almost always are civilians and system operators who are involved by circumstance.

Defying Terrorism

The tactical and strategic value of resilience as a counterterrorism imperative was reinforced in a report, *Assessing the Terrorist Threat*, released September 10, 2010, by the National Security Preparedness Group. According to the report, the diversifying nature of the terrorist threat has been motivated in part by the recognition that attacks on the West—and especially on the United States—do not have to be spectacular or catastrophic to be effective.

As the attempted bombing of Northwest Airlines Flight 563 on Christmas Day 2009 illustrated, even near-miss attacks can generate political fallout and a rush to impose expensive and economically disruptive protective measures. Moreover, recruiting terrorist operatives, even from the targeted societies, is easier for small and unsophisticated attacks.

Changes in Profiles

Terrorist radicalization and recruitment is growing, with groups operating and training at an array of bases worldwide. The profile of a terrorist is no longer clear. Many recruits are radicalized via the Internet, suggesting that the ranks will continue to be filled. The only common denominators among operatives drawn from Western countries appear to be a new-found hatred for their native or adopted land; a degree of dangerous malleability; and a religious fervor that can impel them to potentially lethal acts of violence.

The diversity of recent terrorist recruits presents new challenges for intelligence and law enforcement agencies, already inundated with information and leads. Sophisticated attacks such as those carried out on New York and Washington, D.C., on September 11, 2001, require a larger group of operatives, communications with overseers and planners, and time to conduct surveillance and rehearse the attack, as well as money, identification documents, safe houses for operatives, and other logistical needs. These in turn create opportunities for detection and interception by intelligence and law enforcement agents.

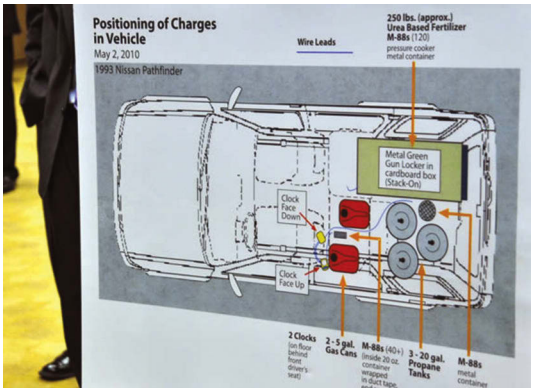
Less sophisticated attacks, in contrast, are almost impossible to prevent. In May 2010, a sidewalk tee-shirt vendor—not the New York Police Department (NYPD) patrolman in a squad car across the street—sounded the alarm about Faisal Shahzad's explosives-laden sport utility vehicle in Times Square. Shahzad was not listed as a suspected terrorist in any federal or NYPD database.

The October 2010 air cargo incident involving explosives hidden in ink cartridges shipped from Yemen is consistent with this trend, with the added goal of economic disruption. The would-be bombers did not know if the cartridges would end up on a commercial airliner with hundreds of passengers or on an air cargo carrier with a small crew. They understood, however, that destroying any plane in midair would trigger a costly and disruptive response that would undermine the movement of global air cargo.

PHOTO: WIKIMEDIA COMMONS

Natural disasters can have extensive impacts. Volcanic ash clouds roll over Bergen, Norway, after the 2010 eruption of Eyjafjallajökull volcano—more than 1,000 km away.

PHOTO: CRAIG CRAWFORD, U.S. DEPARTMENT OF JUSTICE



Some terrorist attacks, such as the attempted car bombing in New York City's Times Square in May 2010, have no obvious predictors or clues for law enforcement officials.

Minimizing Attractiveness

Given these trends, investing in the means to sustain critical functions and improve response to—and rapid recovery from—attacks has tactical and strategic value. Attacks with limited potential to disrupt a society become less attractive to carry out.

The May 1, 2011, killing of Osama bin Laden will not put an end to attacks on innocent civilians and critical infrastructure on U.S. soil; nevertheless, demonstrating the ability to withstand terrorist attacks without sustaining damage to the American way of life makes terrorism a less attractive weapon for U.S. adversaries. Alternatively, a lack of resilience that results in unnecessary loss of life, destruction of property, and the disruption of key networks and functions presents a strategic vulnerability, as long as nonstate actors wage their battles in the civil and economic space instead of in conventional military spaces.

Mitigating Natural Disaster

Most natural disasters and large-scale accidents are more routine than people acknowledge. Although individuals and community and corporate leaders often regard disasters as chance and fate, the risk of disaster is generally predictable.

In addition, the overwhelming costs of disasters almost always are associated with failures of preparation. Losses and damages rise exponentially when risk mitigation measures to assure adequate robustness are not in place, when responses to disasters are poorly planned and executed, and when efforts to speed recovery and implement lessons learned receive minimal attention.

PHOTO: JACE ANDERSON, FEDERAL EMERGENCY MANAGEMENT AGENCY

In May 2011, a tornado leveled homes and other buildings in Joplin, Missouri. Although natural disasters are not uncommon, the devastation can have lasting effects on communities.

PHOTO: U.S. COAST GUARD

Fireboat crews battle post-explosion fires on the offshore oil rig *Deepwater Horizon*. Measures to prevent the 2010 oil spill would have been far less costly than the recovery efforts.

Microscale Initiatives

On the microscale, making an up-front investment in safeguards that mitigate risk and consequences is far more cost-effective than paying for response and recovery after a foreseeable hazard. The *Deepwater Horizon* disaster in the Gulf of Mexico in 2010 illustrates this point. Inadequate attention to preventive measures and the lack of planning for dealing with what was viewed as a low-probability event led to a massive ecological disaster and a significant disruption of the offshore drilling industry.

The failure of the crucial emergency vents at Japan's Fukushima Daiichi nuclear facility after the March 2011 earthquake and tsunami provides another compelling example. The hydrogen explosions after the loss of power rendered the vents inoperable and triggered more than a local nuclear disaster, as consequences cascaded to international transportation networks, global supply chains, and worldwide investments in new nuclear power plants.

Macroscale Initiatives

On the macroscale, a society's level of resilience contributes to its global competitiveness. Pandemics, earthquakes and volcanoes, and more frequent and destructive storms associated with climate change are standing threats. In addition, as witnessed in the near meltdown of global financial markets in the fall of 2008, increasingly complex and interdependent networks support global economic activity, so that problems in one part of the system can quickly produce consequences across the entire system.

The countries, communities, and systems that are most able to manage these risks and bounce back quickly will be the places that people will want to live, work, and invest. Those unable to respond effectively to familiar and emerging risks will become national and global backwaters.

Building Resilience

U.S. policy makers and elected officials generally have overlooked the extent to which decisions about infrastructure investment, design, and regulation play a role in elevating or dampening the risk and impact of a terrorist attack or the effects of a natural disaster. Yet these provide an opportunity and a compelling rationale for investing in infrastructure and ensuring that new projects incorporate measures to mitigate the risk and consequence of man-made and natural disasters.

Almost daily, media reports make clear the consequences of the deferred maintenance and repair of old and overstressed infrastructure. Congested highways, seaports, and airports; bridge collapses; and a passenger rail system that is decades behind the rest of the developed world are evidence that the United States is neglecting a national transportation system that once was the envy of the world. In addition, the power grid cannot handle seasonal rises in temperature, and old pipelines under residential areas are failing.

A new emphasis on building resilience can help change the public's lack of enthusiasm for stepped-up investments in the critical foundations of an advanced society. Resilience can provide safety and security, as well as bolster competitiveness. In creating the Interstate Highway System, President Dwight D. Eisenhower highlighted the national defense value that the system could provide in supporting rapid mobilization and urban evacuation.

Federal Role

Embedding resilience into infrastructure requires specific measures and actions. For the most part, the expertise for developing the measures and actions, as well as the capacity for carrying them out, do not lie within the federal government but with the owners and operators of the nation's infrastructure, who are able to identify and mitigate vulnerabilities in the systems they run. The information and intelligence about threats to infrastructure, however, lie almost exclusively within the federal government, which is reluctant to share findings that could end up in the wrong hands.

The federal government is working to cooperate with the private sector. In 2010, the Department of Homeland Security's Office of Infrastructure Protection established the Engagement Working Group to share classified information with representatives of the private sector to develop strategies for countering threats to infrastructure. The flaw in this commendable program is that federal officials can provide security information only to vetted company security officers, who in turn are barred from relaying the information to executives and managers who do not have active security clearances.

As a result, investment and operational decisions often are made with little attention to security. Furthermore, federal officials miss out on critical insights and perspectives from corporate financial and operational experts. Countering natural and man-made threats effectively and efficiently requires an open dialogue and the implementation of cooperative, public–private, practitioner-guided programs to build infrastructure resilience.

Bridging Theory to Practice

The Port Authority of New York and New Jersey's Applied Center of Excellence for Infrastructure Resilience (ACEIR) offers a promising model for a cooperative, practitioner-guided infrastructure resilience process. When the Department of Home-

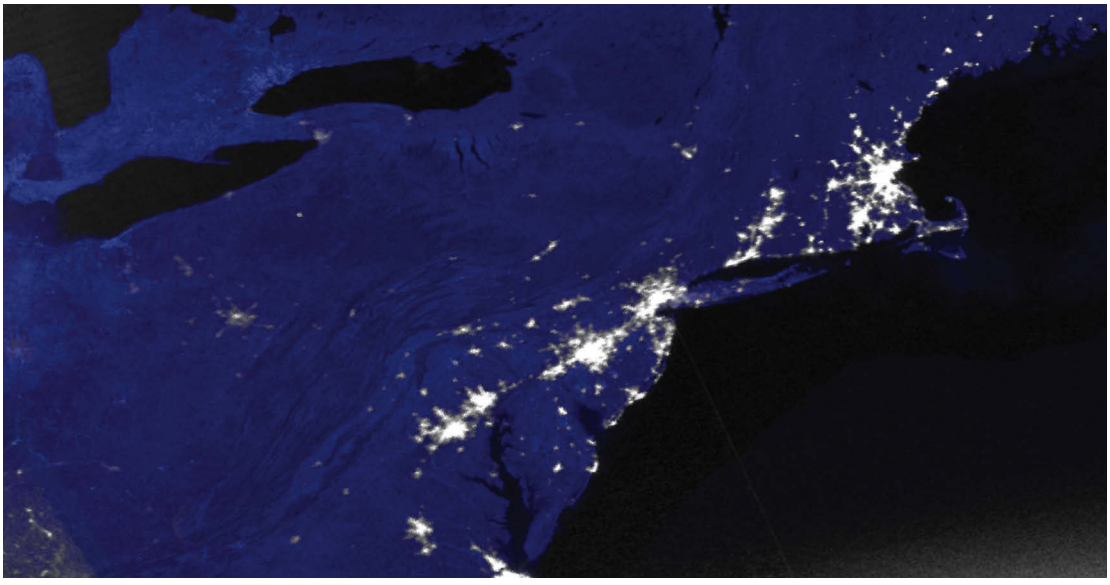


Photo: National Oceanic and Atmospheric Administration

The consequences of deferred routine infrastructure maintenance can be drastic. A cascading blackout that originated in the Ohio area in 2003 caused the loss of power for more than 40 million people across the Northeastern and Midwestern United States and parts of Canada. A nighttime satellite photo shows the darkened regions at left—southern Canada, Ohio, Michigan, Pennsylvania, and parts of New York and New Jersey.

land Security was formed in 2003, it chartered 12 academic centers of excellence to foster multidisciplinary research in security technologies and processes and to provide thought leadership on security policy.

The important next step is to test and validate solutions in a demanding operational environment. The White House National Security Strategy, released in 2010, calls for employing innovative technology and processes through new, strong, and flexible public–private partnerships to create next-generation, resilient infrastructure. Through ACEIR, the Port Authority—the nation's largest infrastructure owner and operator—is forging that kind of partnership, dedicated to bridging theory to practical application.

Metropolitan New York offers an ideal environment for developing and testing infrastructure resilience measures. The Port Authority's facilities support the movement of people and goods in one of the world's most densely populated and commercially active regions. The facilities are diverse, including the World Trade Center site and multimodal transportation systems—tunnels, bridges, bus terminals, airports, maritime facilities, and mass transit rail—that cross state borders. Concepts can be tested in an environment in which they must be effective—at the intersection of critical infrastructure interdependencies.

The Port Authority can subject promising technologies and processes to a demanding operational volume and velocity challenges. Those that hold up under the enormous operational stress of New York systems are likely to work well nationwide. Infrastructure operators would know that these tools and practices have little risk of failure in their urban areas.

Since the summer of 2010, ACEIR has been preparing to serve as a real-world test platform for technological applications and processes. The center will ensure that research projects are vetted by

Five Fundamental, Go-To Documents

Essential Security-Related Titles for Transportation Agencies

JOE CROSSETT

Surface transportation agencies are uniquely positioned to take swift and direct action to protect lives and property—the agencies have broad policy responsibility, public accountability, large and distributed workforces, heavy equipment, and a robust communications infrastructure. This institutional heft also provides a stable base for campaigns to mitigate or reduce risk exposure through all-hazards capital investments.

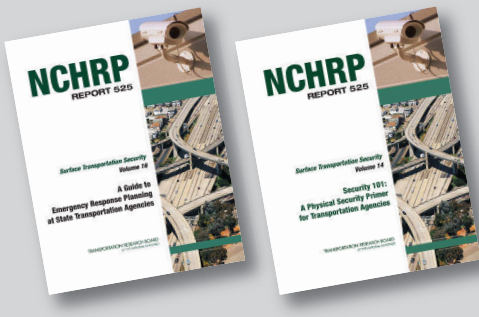
The Transportation Research Board's Cooperative Research Programs are assisting transportation agencies in adopting the National Incident Management System (NIMS) framework. In a September 8, 2004, letter to state governors, Tom Ridge, then Secretary of the Department of Homeland Security, wrote that "NIMS provides a consistent nationwide approach for federal, state, territorial, tribal, and local governments to work effectively and efficiently together to prepare for, prevent, respond to, and recover from domestic incidents, regardless of cause, size, or complexity."

The American Association of State Highway and Transportation Officials' (AASHTO) Special Committee on Transportation Security and Emergency Management (SCOTSEM) and the American Public Transportation Association's (APTA) Executive Committee Security Affairs Steering Committee provide direction to CRP security research. A technical panel provides all-hazards, all-modes oversight and project selection guidance through National Cooperative Highway Research Program (NCHRP) Project 20-59, Surface Transportation Security Research.

The list of completed CRP-sponsored research products is ever increasing. After a review of the 86 CRP research projects completed as of October 2010, a report prepared for AASHTO SCOTSEM identified a suite of five fundamental, go-to documents for transportation agencies. Each report tackles a critical emergency management or transportation security topic and offers readily implementable, comprehensive, and up-to-date guidance for the major elements of a state's all-hazards transportation security and emergency management program.

◆ ***A Guide to Emergency Response Planning at State Transportation Agencies***, NCHRP Report 525, Volume 16 (2010). Emergency response planning is a wide-ranging topic applicable to every state department of transportation (DOT). The NCHRP guide is the only comprehensive resource available on state-of-the-art emergency response planning practices at state DOTs. The guide examines the institutional context for emergency response planning and explains how surface transportation agencies can develop a program to plan, prepare for, respond to, and recover from a range of hazards and threats. (For more information about the book, see the article by Wallace on page 27.)

◆ ***Security 101: A Physical Security Primer for Transportation Agencies,*** NCHRP Report 525, Volume 14 (2009). An introductory-level reference



front-line operators, engineers, and managers and that results are evaluated by a board of advisers, who are internationally respected practitioners and academics. Eventually ACEIR can provide a venue for industry input into federal research and development projects. In addition to evaluating projects developed by federal agencies, the ACEIR board of advisers could identify research needs. Although still in its formative stages, ACEIR can serve as a model for other infrastructure sectors.

Ailing Infrastructure

Efforts to advance infrastructure resilience must ensure that investments to extend the service life of infrastructure systems will integrate measures addressing continuity in the face of disruptions. In 2008, the American Society of Civil Engineers evaluated the nation's infrastructure with a grade of D and identified an investment gap of more than $2 trillion for the repair of roads, bridges, ports, and other critical facilities and systems. The tab cannot be put off indefinitely. When the nation attends to its ailing foundations, it will have an historic opportunity to incorporate measures for resilience in response to man-made and natural disturbances.

The United States is in the formative stages of crafting the means to secure infrastructure and build resilient infrastructure systems. The most serious challenge involves the interdependencies among infrastructure sectors. No system operates in isolation, and because these interdependencies are vast and complicated, they are best understood not at the national level, but within regions and communities.

Tools and Incentives

Developing resilient infrastructure systems, therefore, must proceed from the bottom up. Advancing resilience at the community level, however, requires

document designed to enhance transportation professionals' working knowledge of security practices, the primer provides a timely and comprehensive resource for DOTs seeking basic information about current and accepted practices for ensuring the physical security of personnel and surface transportation assets. (See the article by Frazier on page 10 for more information about the book.)

◆ ***Blast-Resistant Highway Bridges: Design and Detailing Guidelines,*** NCHRP Report 645 (2010). The impacts of explosive loads on buildings and military structures have been studied for many years, but design for resistance to explosive effects is a new area for bridge engineers. The only comprehensive resource on this topic for state DOTs, the report provides design guidance for improving the structural performance of bridges in response to explosive loads, using the AASHTO load and resistance factor design format familiar to bridge engineers. (For more information about the book, see the discussion in the feature article on page 12.)

◆ ***Costing Asset Protection: An All-Hazards Guide for Transportation Agencies (CAPTA),*** NCHRP Report 525, Volume 15 (2009). The CAPTA report and a Microsoft Excel planning tool help transportation agencies make systemwide decisions about capital and operating budget allocations across modes, based on information about vulnerabilities in individual transportation assets that could cause significant losses. (For more information, see the article by Scanlon on page 16.)

◆ ***Continuity of Operations Planning (COOP) Guidelines for Transportation Agencies,*** TCRP Report 86, Vol. 8, and NCHRP Report 525, Vol. 8 (2005). The multimodal guidelines in this report assist state and local highway and transit agencies in developing, implementing, maintaining, training for, and exercising COOP capabilities. The research for this report has produced several practical deployment strategies, including downloadable worksheets, a template for COOP, a series of brochures explaining the COOP process to staff, a customizable Microsoft PowerPoint presentation, and more than 300 resource documents constituting an electronic library on the topic.

Many state DOTs and public transportation agencies have emergency response plans that address immediate operational situations but do not include contingencies for carrying out plans from alternative facilities or for an extended period. COOP helps transportation agencies ensure the performance of critical services in an operating environment that is threatened, diminished, or incapacitated. Although the COOP guidelines are not new, this report is the only comprehensive resource available for state DOTs about state-of-the-art COOP practices.

Capsule descriptions of the full array of CRP security-related products and links to a variety of products and resources on security, emergency management, and infrastructure protection produced by TRB, other divisions of the National Research Council, and other transportation research organizations can be found at www.TRB.org/SecurityPubs.

The author is Partner, High Street Consulting Group, LLC, Pittsburgh, Pennsylvania.

that civic and business leaders have the tools, a way to measure progress, and clear benefits from reaching a recognized standard.

One reward may be to provide communities with better bond ratings and lower insurance premiums for demonstrating that they have adopted measures to reduce the risk of damages and to improve the speed of recovery. But recruiting the insurance industry as an ally in dealing with the risk of catastrophic events poses three challenges:

- Insurers tend to steer away from arrangements that may involve ruinous losses and insolvency;
- Insurers require a broad pool of policyholders to diversify the risk and would need to be confident that enough customers would buy their product; and
- Private insurance companies need to be confident that the measures they would be subsidizing through reduced premiums will mitigate risk effectively and that their clients are adopting the measures.

Federal and state governments can lower or eliminate each of these barriers for insurers. For instance, government could cap the risk that insurance companies face and could agree to make up the difference to the policyholder if the losses exceed the cap. The government also can help assure an adequate pool of customers for the insurance companies by providing a tax break to insurers who write new policies or by providing grants to communities to subsidize the initial premiums. Finally, the government can establish and reinforce the standards against which the insurance incentive is set.

Community-Level Model

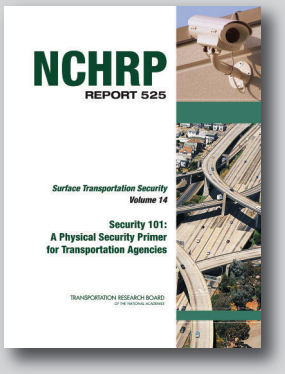
The Community and Regional Resilience Institute (CARRI) at Oak Ridge National Laboratory has developed a promising model for deepening private–public cooperation and aligning financial incentives for building and maintaining preparedness at the local level. CARRI has led an effort to define the

Security 101

Primer on Protecting Agency Personnel and Assets

ERNEST R. FRAZIER, SR.

Security 101: A Physical Security Primer for Transportation Agencies (NCHRP Report 525, Volume 14) assembles basic information about current and accepted practices for ensuring the physical security of personnel and assets for departments of transportation, transit agencies, and motorcoach service providers. The introductory reference includes information about security practices and explores their applicability to surface transportation.



The text primarily addresses transportation personnel who do not have backgrounds in security but who must address, perform, or supervise security activities as a part of their job responsibilities. The report, however, is sufficiently detailed to function as a reference for security professionals as well.

The focus is on measures and concepts to safeguard personnel and to protect equipment, installations, materiel, and documents against espionage, sabotage, damage, and theft. The report covers security risk management and threat assessment techniques, security plan development, tools and countermeasures, training, setting priorities for asset protection, and integrating federal homeland security practices.

Security 101 offers transportation agencies a comprehensive approach to enhancing physical security organizationwide. The primer contains visual aids and graphics, plus four appendices: a 31-page annotated bibliography; more than 100 additional references; more than 1,000 security-related acronyms and abbreviations compiled from a literature review; and definitions of more than 1,000 security-related terms—many of which have more than one definition, reflecting the range of source documents for the state of the practice.

Plans are to use *Security 101* as the primary text for a series of regional workshops for transportation agencies about basic physical security concepts, enhancing working relationships with security partners, and identifying opportunities to improve physical security practices.

NCHRP Report 525, Volume 14, *Security 101: A Physical Security Primer for Transportation Agencies*, is available online at www.TRB.org/SecurityPubs/; to purchase a print copy, go to the TRB online bookstore, www.trb.org/Finance/Bookstore.aspx.

The author, an attorney, is principal, Countermeasures Assessment & Security Experts, LLC, New Castle, Delaware, and is the retired Chief of Police for Amtrak. He is the author of NCHRP Report 525, Volume 14, Security 101: A Physical Security Primer for Transportation Agencies.

parameters of resilience, modeled on the creation of the fire and building codes more than a century ago.

Drawing on a two-year prototype effort undertaken in Charleston, South Carolina; Gulfport, Mississippi; and Memphis, Tennessee, the Community Resilience System Initiative set out to identify the policies, practices, and capabilities that can increase the likelihood that communities will maintain essential functions with little disruption or, when disrupted, will recover the functions rapidly and with minimal loss of economic and social value.

To accomplish this, the initiative sought to help community stakeholders understand

1. What characterizes resilience,
2. How to assess resilience,
3. How to prioritize options for improving resilience,
4. How to measure the impact of the improvements objectively, and
5. How to develop rewards for investments.

After two years of field research, CARRI spent an additional 18 months to convene a network of former governors, former and current mayors, emergency planners, finance and insurance executives, representatives from government agencies, and academics to develop detailed guidelines and comprehensive resources to assist communities in devising resilience plans. These insights are embedded in a web-enabled tool, which can be modified and upgraded quickly as new lessons are learned. Five communities across the United States will test the web tool this fall.

The system is designed to enable local leaders to assess their community's resilience, plan to increase the resilience, implement and sustain the plans, and evaluate and revise the plans as needed. The system includes a focus on infrastructure, infusing the approach with the kind of local knowledge and expertise that will be replicable and adoptable by other communities nationwide.

Social Benefit of Resilience

Making resilience a national imperative reinforces what unites a society, not what divides it. Building resilience is not possible without substantial collaboration and cooperation at all levels of a society. Individuals must develop the means to withstand, recover rapidly from, and adapt to the risks they encounter at the personal and family level. Companies and communities must look within and beyond their bounds to ensure that they are prepared to handle what may occur as a result of internally and externally generated risks. Finally, at the national level, the emphasis on resilience highlights the necessity for forging relationships and developing protocols for dealing with shared risks.

In short, the determination to confront ongoing exposure to catastrophic man-made and natural disasters is not an act of pessimism or paranoia, nor is it inherently a cost center. The effort involves a mature recognition that things go wrong from time to time and that preparations serve as a reminder not to take things that are important and critical for granted.

Photo: Richard David Ramsey

The Friendship Oak, a live oak tree in Gulfport Mississippi, is more than 500 years old and survived the devastation of Hurricane Katrina in 2005.

Symbol of Resilience

A dramatic symbol of resilience stands just outside of Gulfport, Mississippi, a few hundred yards from the Gulf of Mexico, in an area devastated by Hurricane Katrina in August 2005—a live oak tree known as the Friendship Oak. The tree is approximately 50 feet tall with a trunk that measures about 18 feet in circumference, deep and sprawling roots, and branches that stretch out 150 feet. The Friendship Oak has stood sentinel for more than 500 years.

Live oaks are nature's models of resilience, adapted to their environment by developing the capacity to withstand what comes their way. When ships were built of wood, lumber from live oaks was the most sought-after material for the curved portions of a vessel's hull, which required maximum strength.

The live oak offers a guide for managing the risk of terrorism and disaster in local American communities and nationwide: like these magnificent trees, adapt and grow to cope with what will inevitably come but also be able to stand tall, confident, and true to individual and national potential.