TR News July-August 2011: Security and Critical Infrastructure Protection

DETAILS

60 pages | | PAPERBACK

ISBN 978-0-309-43106-4 | DOI 10.17226/22854

AUTHORS

TR NEWS

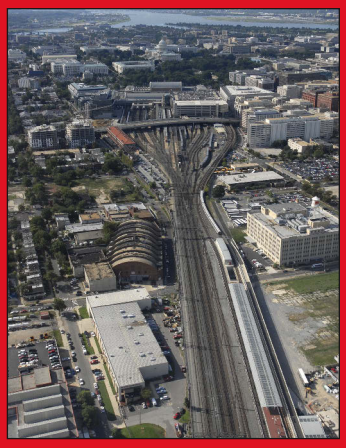
NUMBER 275 JULY–AUGUST 2011

SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

4

12

37



COVER: Union Station in Washington, D.C., near the U.S. Capitol; security in transportation demands attention to infrastructure resilience, design, and vulnerabilities. (Photo: Larry Levine, Washington Metropolitan Area Transit Authority)

TR NEWS

features articles on innovative and timely research and development activities in all modes of transportation. Brief news items of interest to the transportation community are also included, along with profiles of transportation professionals, meeting announcements, summaries of new publications, and news of Transportation Research Board activities.

***TR News* is produced by the Transportation Research Board Publications Office**
Javy Awan, Editor and Publications Director
Lea Camarda, Assistant Editor
Jennifer J. Weeks, Photo Researcher
Juanita Green, Production Manager
Michelle Wandres, Graphic Designer

TR News (ISSN 0738-6826) is issued bimonthly by the Transportation Research Board, National Research Council, 500 Fifth Street, NW, Washington, DC 20001. Internet address: www.TRB.org.

Editorial Correspondence: By mail to the Publications Office, Transportation Research Board, 500 Fifth Street, NW, Washington, DC 20001, by telephone 202-334-2972, by fax 202-334-3495, or by e-mail jawan@nas.edu.

Subscriptions: North America: 1 year $55; single issue $10. Overseas: 1 year $80; single issue $14. Inquiries or communications concerning new subscriptions, subscription problems, or single-copy sales should be addressed to the Business Office at the address below, or telephone 202-334-3216, fax 202-334-2519. Periodicals postage paid at Washington, D.C.

Postmaster: Send changes of address to *TR News*, Transportation Research Board, 500 Fifth Street, NW, Washington, DC 20001.

COMING NEXT ISSUE

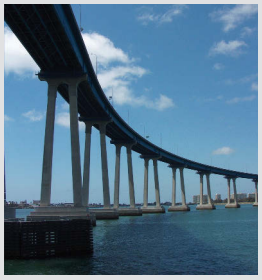
PHOTO: AIRPORTS COUNCIL INTERNATIONAL–NORTH AMERICA

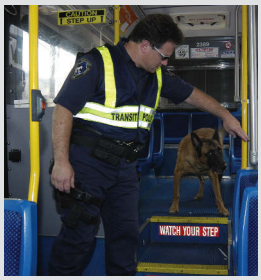
Experimental technology to assist in navigation; the aviation industry is undergoing rapid changes and is testing innovations at all levels.

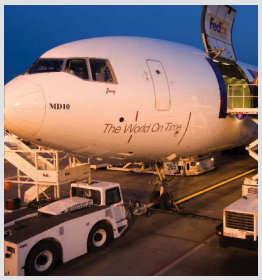
The magazine's first-ever theme issue on aviation topics is getting ready for takeoff, with a cargo of feature articles covering the Next-Generation Air Transport System, which will transform U.S. air traffic control from a ground-based, human-centric system to a satellite-based, airplane-centric system; the future of aviation sustainability; commercial aviation's pursuit of sustainable alternative fuels; aviation security; economics of the aviation industry; and more.

INTRODUCTION

SECURITY & CRITICAL INFRASTRUCTURE PROTECTION







Progress and Paths to Resilience

The effects of the terrorist attacks of September 11, 2001 (9/11), reverberate through each of the articles in this special issue on transportation security and critical infrastructure protection. Each article offers positive, practical solutions, responses, and approaches based on research findings in the past 10 years, to prevent similar attacks and to mitigate the effects of attacks if prevention fails.

This is the fourth issue of the magazine devoted to transportation security.[1] The magazine's first theme issue on the topic came out almost one year before the 9/11 attacks, in November–December 2000, and received accolades for its pioneering, concentrated coverage of the topic. But the issue was more than pioneering—it was prophetic, as the lead article presented a scenario in which Osama Bin Laden used a mode of transportation to trigger mass destruction inside U.S. borders—although the scenario hypothesized an intermodal container transported inland from a port via rail. The author of that article, Stephen Flynn, is coauthor with Sean Burke of the lead feature in this issue, presenting the urgent case for infrastructure resiliency and renewal. The need for resilience, which not only enables quick recovery but also serves as a deterrent, is a recurring theme in the accompanying articles.

Another recurring theme is the practical research undertaken through the Transportation Research Board's Cooperative Research Programs at the specific request of federal, state, and transportation agency sponsors, developing guidance, toolkits, and procedures. Many of these are highlighted in brief articles, often by the principal investigators, but also come into the spotlight in the feature articles by Eric L. Sammarco, Eric B. Williamson, and Carrie E. Davis on developing specifications to protect bridges and by Yuko J. Nakanishi on the array of measures to protect U.S. transit systems.

Three feature articles consider the ramifications of security policies in the past decade: for aviation security—a topic always in the headlines—by Richard W. Bloom; on Canada–U.S. trade, vital for both nations' economic recoveries, by Mary R. Brooks; and on maritime security and the global supply chain—which faces threats far more serious than that of piracy—by Stephen Carmel.

One author, Joseph Scanlon, reports that a National Cooperative Highway Research Program panel overseeing a project to develop an all-hazards guide for transportation agencies came to the realization that "the source of the threat was only one issue—the loss of an asset has the same consequence whatever the cause of the loss." Security involves the protection of critical transportation infrastructure and is linked to the pressing issue of infrastructure renewal.

—Joedy Cambridge and Stephan A. Parker
Transportation Research Board

[1] *TR News* 211, November–December 2000, Transportation Security: Protecting the System from Attack and Theft; *TR News* 238, May–June 2005, Transportation Security Training and Education: Resources, Techniques, and Strategies; *TR News* 250, May–June 2007, All-Hazards Preparedness, Response, and Recovery.

EDITOR'S NOTE: Special thanks and appreciation are expressed to TRB Senior Program Officers Joedy Cambridge and Stephan A. Parker for their contributions in developing this issue of *TR News*. Cambridge assembled two of the three previous security theme issues of the magazine and recruited several feature articles on the topic for other issues; Parker also developed an earlier theme issue and manages TRB's living library of security-related research and resources.

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.

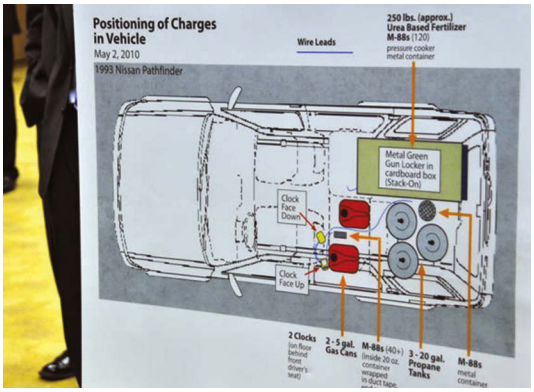
Less sophisticated attacks, in contrast, are almost impossible to prevent. In May 2010, a sidewalk tee-shirt vendor—not the New York Police Department (NYPD) patrolman in a squad car across the street—sounded the alarm about Faisal Shahzad's explosives-laden sport utility vehicle in Times Square. Shahzad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

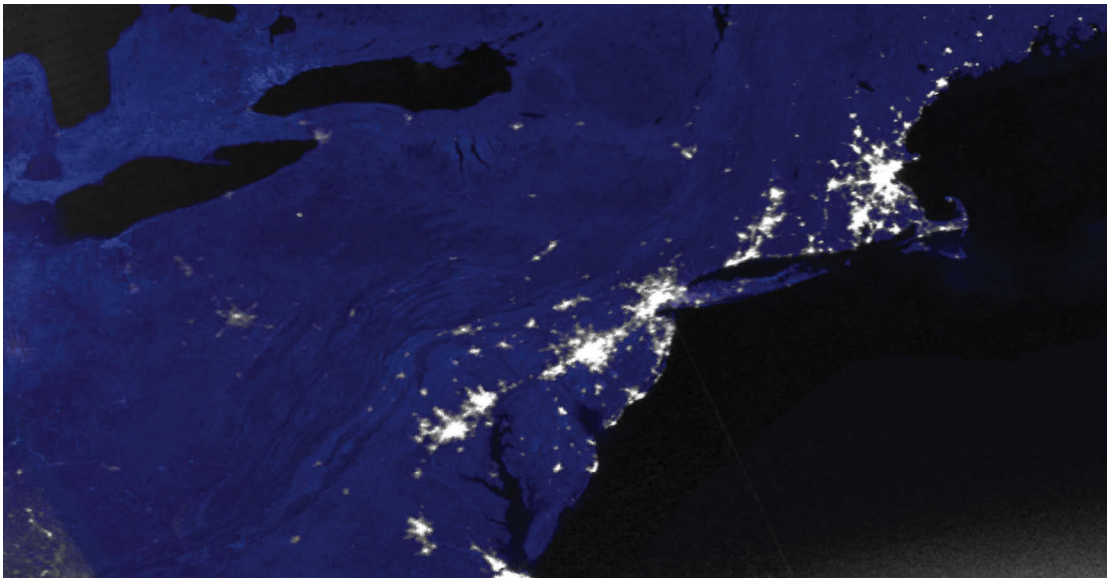


Photo: National Oceanic and Atmospheric Administration

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

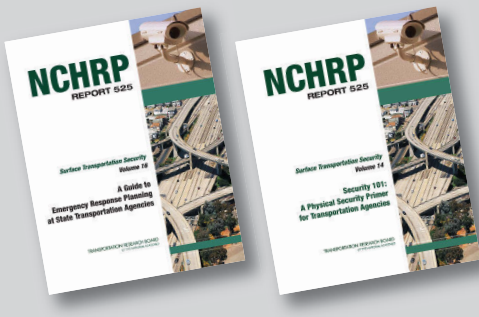
Surface transportation agencies are uniquely positioned to take swift and direct action to protect lives and property—the agencies have broad policy responsibility, public accountability, large and distributed workforces, heavy equipment, and a robust communications infrastructure. This institutional 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

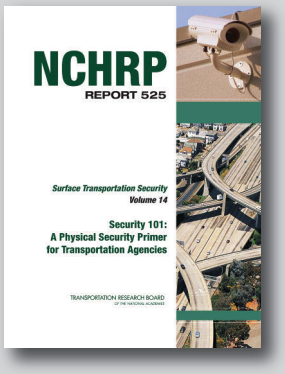
The Community and Regional Resilience Institute (CARRI) at Oak Ridge National Laboratory has developed a promising model for deepening private–public cooperation and aligning financial incentives for building and maintaining preparedness at the local level. CARRI has led an effort to define the

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 organization-wide. 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.

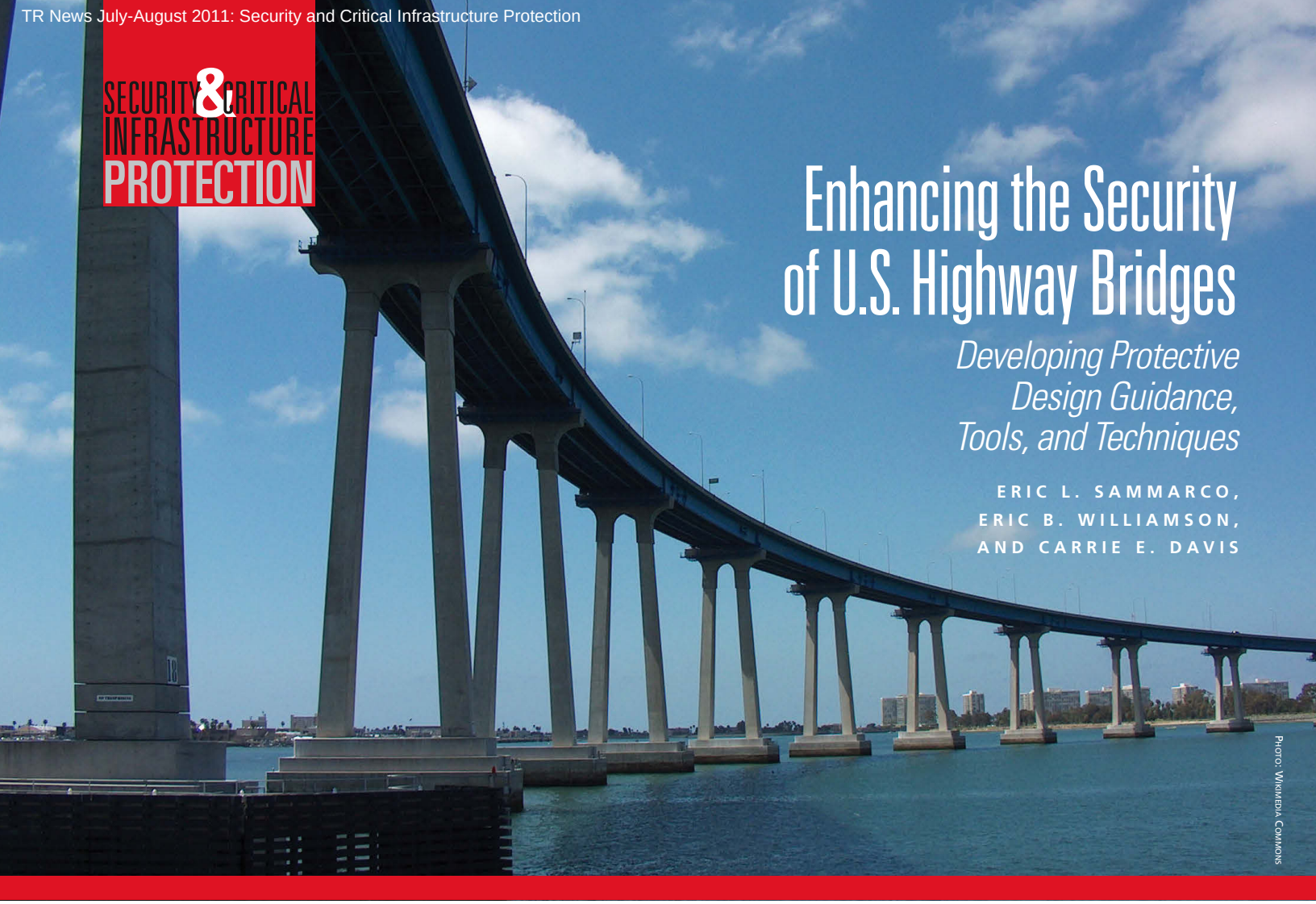
Symbol of Resilience

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.

SECURITY & CRITICAL INFRASTRUCTURE PROTECTION



Enhancing the Security of U.S. Highway Bridges

Developing Protective Design Guidance, Tools, and Techniques

ERIC L. SAMMARCO, ERIC B. WILLIAMSON, AND CARRIE E. DAVIS

PHOTO: WIKIMEDIA COMMONS

Sammarco is a doctoral student, and Williamson is Associate Professor, Civil, Architectural, and Environmental Engineering, University of Texas at Austin; and Davis is Research Engineer, Protection Engineering Consultants, Austin.

The San Diego–Coronado Bridge in California was the site of a bomb scare in May 2011. U.S. intelligence indicates that the potential is high for attacks to highway infrastructure.

A large-scale terrorist attack against a major U.S. highway bridge was thought highly unlikely a little more than a decade ago, when the nation shared an "it will never happen here" attitude. Construction drawings and design details for major transportation infrastructure were available to the public, and major bridge design codes lacked provisions addressing protective design. The terrorist attacks of September 11, 2001 (9/11), revealed the vulnerability of the nation's infrastructure, and subsequent examinations have raised major concerns about highway bridge security in the United States.

Documented Trend

The 9/11 terrorist attacks on the World Trade Center and the Pentagon produced thousands of fatalities, extensive economic losses, and fear and anxiety nationwide. International terrorist organizations have been active across the globe for decades, but attacks on public surface transportation infrastructure constitute a recent trend. The number of documented terrorist attacks against these targets increased from fewer than 20 in 1985 to nearly 120 in 2003 and 2004 (*1*).

The Mineta Transportation Institute (MTI) has documented 1,633 worldwide terrorist attacks against public surface transportation infrastructure as of the first quarter of 2010—161 targeted highway infrastructure, and 82 of these involved explosives or incendiaries.

Although the 1977 explosion on the Route 1 Bridge in Florida Homestead and Key West is the only U.S. highway infrastructure attack documented in MTI's database, intelligence gathered from captured terrorists and threats received by U.S. authorities suggest that the potential for future attacks is high. Between 1977 and the turn of the century, the United States received six major bomb threats to public highway infrastructure; half of these targeted noniconic structures—that is, typical highway bridges (*1, 2*).

In May 2000, an Al Qaeda training manual seized by police in Manchester, England, included missions to gather information for blasting and destroying bridges leading into and out of major cities (*3*). In 2003, a captured Al Qaeda leader revealed that a bridge in California was on a list of possible targets (*3*). Mohammed Rauf, an Al Qaeda operative, was arrested in June 2003 for plotting to destroy the

Brooklyn Bridge and admitted to plans for simultaneous terrorist attacks on New York City and Washington, D.C.

In April 2004, a bridge operator discovered a package secured to a main bridge girder with bungee cords on the Bay St. Louis Bridge in Mississippi and notified the U.S. Coast Guard. The package enclosed a plastic container housing a brown box with wires sticking out (*4*). Yet another bomb threat to the Brooklyn Bridge occurred in October 2010, when a flashlight was discovered connected by copper wiring to packages on each side of the bridge deck.

Worldwide historical data, however, suggest that terrorists tend to attack noniconic transportation infrastructure. Two detailed chronologies addressing a sample of the MTI database indicate that more than half of the documented attacks on public highway bridges have been associated with noniconic structures (*2, 5*). This finding raises concern, because major U.S. bridge specifications contain little or no guidance for protective design.

Addressing Vulnerabilities

The vulnerability of the U.S. highway bridge inventory has become an urgent issue. The main structural components of a bridge are exposed to the environment. Furthermore, the ability to impose physical standoff—that is, the distance between an explosive and the target—through deterrent systems such as barriers, bollards, or landscaping, or through controlled access points, is limited.

As a result, a terrorist could place a large explosive device close to a critical structural component of a major U.S. highway bridge. Buildings typically have more structural members than bridges and therefore have greater system redundancy; consequently, bridges have less ability to withstand extensive localized damage.

To address these vulnerabilities, researchers and highway transportation authorities have applied risk management and risk-based threat mitigation methodologies to aid in the planning and design of new highway bridges and to facilitate retrofits. A comprehensive approach to integrate protective design concepts and guidance into new highway bridges would include site layout recommendations, active and passive deterrence options, performance-based bridge design standards, blast load characterization options, structural analysis options, blast-resistant design concepts, and retrofit guidance (*6*).

Approaches and Tools

Resources are limited, however, and the nation's highway bridge infrastructure is too massive for an across-the-board effort to mitigate terrorist threats. At the request of the American Association of State Highway and Transportation Officials (AASHTO), the National Cooperative Highway Research Program (NCHRP) developed an objective and logical procedure for identifying infrastructure in need of immediate security enhancement and for prioritizing threat mitigation for bridges (*7*).

The U.S. Army Engineer Research and Development Center combined the AASHTO-NCHRP methodology with concepts and procedures from natural hazard risk assessment to develop a risk-based procedure for prioritizing threat mitigation at the component level (*8*). The proposed procedure assigns risk factors to individual bridge components to indicate importance and vulnerabilities. The importance primarily reflects a component's contribution to structural stability, as well as the cost for its replacement or repair. Vulnerability is a function of a threat's type, size, and likelihood and of the component's resistance to the threat.

In addition, NCHRP, the Federal Highway Administration (FHWA), and other organizations have funded research to develop bridge-specific protective design provisions and engineering tools for deployment into practice. Including protective design provisions in bridge specifications will ensure that bridges are capable of resisting blast loads from bulk explosives without a gross loss in load-carrying capacity.

Focus on Columns

Columns are particularly important to the structure of a typical highway bridge. Bridge columns transmit gravity loads from the bridge deck to the foundation, and are essential to lateral load resistance. When local damage occurs to the bridge deck or to supporting girders, the structure's redundancy and ductility can allow internal forces to redistribute, providing an alternative load path and maintaining structural stability. In contrast, extensive damage to a bridge column has great potential to precipitate partial or total collapse.

Bridge columns therefore have been the focus of experimental research programs in the past decade, to characterize the dynamic response of columns under severe blast loads and to develop design guidance to achieve desirable response under extreme loading. This information can contribute to engineering tools that accurately predict the response of bridge columns to a nearby detonation of high explosives.

Two-Phase Study

Researchers at the University of Texas at Austin (UT-

PHOTO: AD MESKENS

The Brooklyn Bridge has been the site of bomb threats both proposed—as by an Al Qaeda operative in 2003—and observed, as when a flashlight was discovered connected to two packages on the bridge deck in 2010.

FIGURE 1 Observed direct shear failure state of column specimen (*9*).

Austin) have worked to develop a national standard for the blast-resistant design of highway bridge columns (*9*). The research involved large-scale blast tests in two phases. The first phase focused on characterizing the behavior of shock waves in the vicinity of slender structural elements, such as bridge columns, and the second phase focused on the response of half-scale reinforced concrete column specimens subjected to small standoff and near-contact bulk explosives.

The Phase 2 half-scale column tests yielded information for developing design criteria for blast-resistant columns. In general, the survivability of the tested bridge columns was governed primarily by the type, placement, and detailing of the transverse reinforcement. Continuous spiral reinforcement performed best; the second-best option used closely spaced and properly anchored discrete hoops or rectilinear ties.

Longitudinal reinforcement splices also played a major role in the survivability of a bridge column. Lap splices near the same elevation as an explosive charge were prone to failure if the column incurred extensive localized damage. Once the integrity of the lap splices was compromised, the damage spread throughout the column. With no lap splices, however, damage was confined to approximately one column diameter above and below the elevation of the explosive charge.

The Phase 2 blast tests also revealed a direct shear failure in some of the columns. Unlike the more common, flexurally induced diagonal-tension shear, direct shear derives from a load or geometric discontinuity—for example, at a support location—and is associated most often with a visible shear slip plane. Figure 1 (above) depicts an observed direct shear failure; the circular column contained moderately spaced, discrete circular hoops that were inadequately anchored into the concrete core.

Testing Seismic Designs and More

Researchers at the State University of New York (SUNY) at Buffalo investigated how columns designed for seismic applications would perform under a blast event (*10*). Funded by FHWA, the program tested four quarter-scale columns: two were seismically detailed, and the other two were not, but were retrofitted with structural steel jackets.

During earlier experiments with cyclic lateral loads representing a seismic event, both column designs exhibited ductile flexural behavior. Results from the experimental blast tests revealed, however, that failure was governed by direct shear near the column base—a nonductile and highly undesirable mode of failure. The SUNY experiment indicated that design provisions derived solely from seismic research should, in general, not be relied on for blast-resistant design.

Additional experiments have undertaken blast testing of other critical bridge components, including prestressed concrete bridge girders (*11*) and structural steel suspension bridge towers (*12*).

Limitations of Blast Tests

Although experimental research has produced insights into the effects of bulk explosives on the structural performance of critical highway bridge components, blast testing has several limitations. The high pressures and temperatures generated near a detonation decrease the survivability of the data acquisition instruments; moreover, the shock wave propagation is highly variable; as a result, determining the time-varying magnitude and the spatial distribution of the blast loads presents a challenge.

In addition, the immense fireball from a high explosive detonation often can prevent a high-speed video camera from recording the dynamic response of a test specimen. Figure 2 (page 15) illustrates the extreme environment associated with a small standoff detonation. Moreover, experimental blast testing is expensive compared with more traditional structural engineering tests involving static loads.

A below-deck detonation, for example, generates a complex airblast environment. As shown in Figure 3 (page 15), the geometry of a typical highway bridge can consist of multiple inclined reflecting surfaces and partially vented cells—both complicate the behavior of propagating shock waves. Researchers therefore have begun to apply computational simulation tools to understand the effects of bulk explosives on the structural performance of critical highway bridge components.

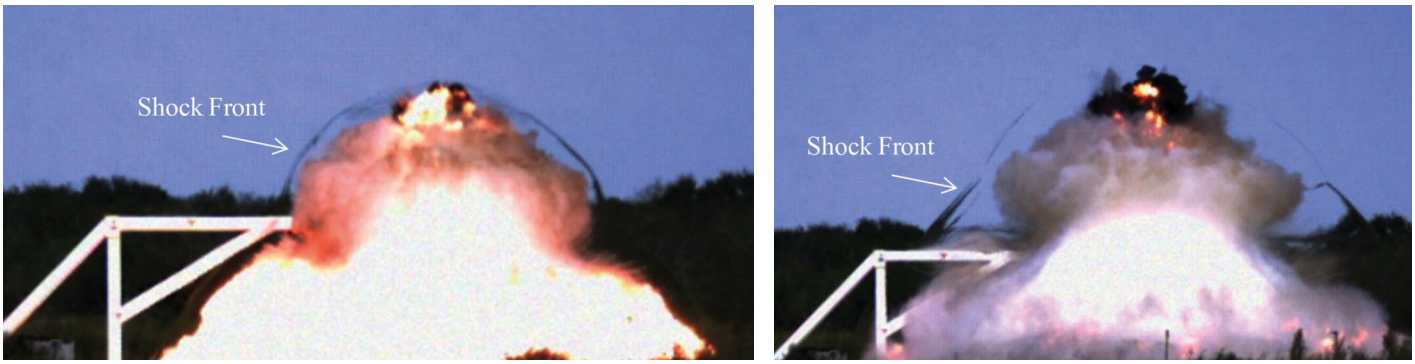


FIGURE 2 Illustration of fireball and shock front from high-explosive detonation.

Computational Research

Several efforts in the past decade have pursued computational research into how blast loads evolve and interact with structural components after a below-deck detonation. For example, researchers at the U.S. Army Engineer Research and Development Center used three different blast load prediction tools to estimate the transient overpressures delivered to the components of a typical highway bridge (*13*).

The researchers also assessed the accuracy and computational cost of each tool and identified the limitations of each:

- Conventional Weapon Effects Predictions (CONWEP), which predicts blast loads on a planar reflecting surface, such as an external wall, from a spherical or hemispherical airburst;
- BlastX, which employs a semiempirical blast load prediction model for shock wave reflections and interactions; and
- Second-Order Hydrodynamic Automatic Mesh Refinement Code (SHAMRC), a high-resolution computational fluid dynamics code for modeling the propagation of shock waves.

CONWEP, the lowest resolution tool, was not capable of incorporating shock wave reflections between multiple surfaces and yielded unconservative results. The medium resolution BlastX tool was able to capture the increased overpressures of multiple shock wave reflections but was not able to capture flow channeling between the bridge girders or the significant pressure stagnation that occurred near the abutments.

SHAMRC yielded the most accurate results but was the most computationally expensive tool, requiring hours of computation with multiple processors running in parallel. The findings emphasized the need for a bridge-specific tool to characterize blast loads and maintain a balance between accuracy and computational cost.

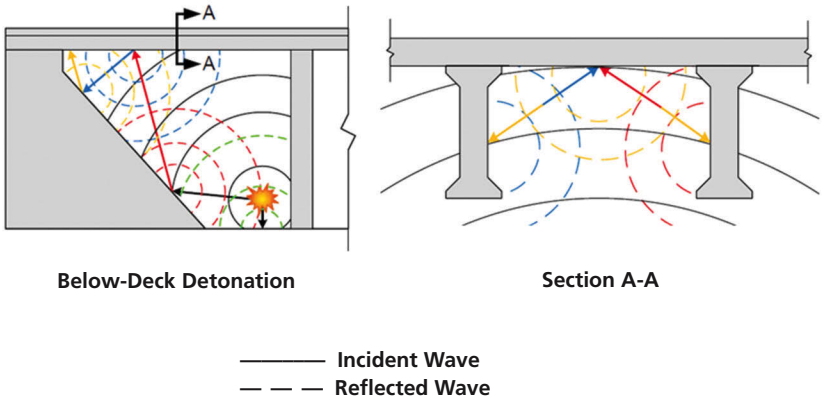
Shock Wave Behavior

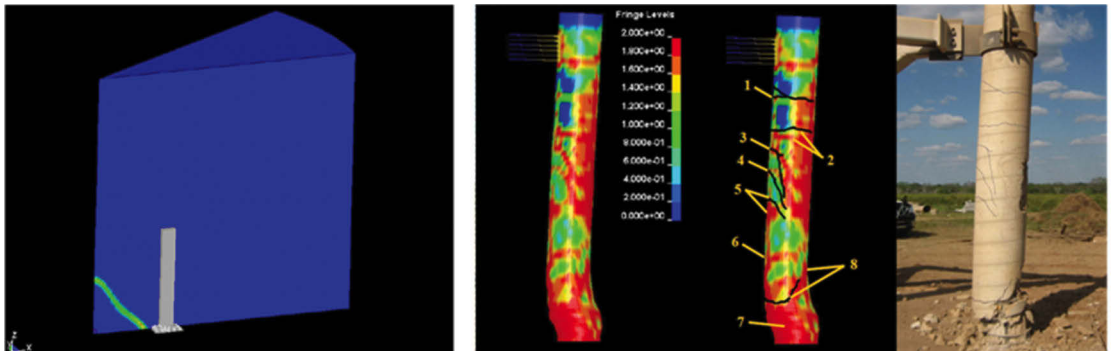
Shock wave behavior in the vicinity of slender structural components is another complex subject well-suited for computational investigation. Experimental blast tests have indicated that blast loads on a large planar reflecting surface—such as the exterior wall of a building—can differ notably from those on a slender structural component, such as a bridge column.

During the NCHRP highway bridge column project, UT-Austin researchers conducted a computational study to characterize this behavior (*9, 14*). Nonlinear finite element analyses were conducted to simulate the experimental blast tests. Figure 4 (page 16) depicts two exercises from the computational study. The computed results aligned with the observations from the experimental blast tests—the enhanced clearing and wraparound pressure effects of slender structural components chiefly reduced the blast loads.

In general, when an incident shock wave emanating away from the explosive source encounters an obstruction, a reflected wave and a refracted wave are generated. This temporarily increases interface pressures, so that the pressures at the extreme edges become larger in magnitude than the adjacent air pressure and expand outward, reducing the effective pressures on the extreme edges. Commonly referred

FIGURE 3 Illustration of airblast complexities from a below-deck detonation.





(a) (b)

FIGURE 4 Computational simulations of airblast tests in NCHRP Project 12-72: (*a*) Phase 1; (*b*) Phase 2 (*14*).

to as clearing, this process continues to propagate toward the center of the reflecting surface until the stagnation pressure is reached. As a result, the wider the reflecting surface, the longer it takes for the relief wave to reach the center, and the longer the reflected pressures act on a reflecting surface, the more severe the loading that a structural component must resist.

The computational study revealed that bridge

Buying Down Risk

Step-by-Step Guide to Cost-Effective Protection of Transportation Assets

JOE SCANLON

Transportation agencies always have faced hazards and threats—accidents, weather, vandalism, and criminal activity—and have learned to handle these in routine fashion. A new set of threats, however, emerged with the September 11, 2001, terrorist attacks—improvised explosive devices and chemical, biological, and radiological attacks.

NCHRP Report 525, Volume 15, *Costing Asset Protection: An All-Hazards Guide for Transportation Agencies (CAPTA)*, assists agencies in identifying these new threats, determining what can be done, and calculating the cost. The report also helps agencies prepare for other severe threats, including natural hazards and extreme weather.

The guide to CAPTA, accompanied by an implementation software package, CAPTool, helps executives of transportation agencies answer questions about extreme events—what assets need protection, what kind of protection, which are most critical, and what are the costs—through rational decisions about expenditures and necessary actions. The text proceeds step by step, evaluating assets, examining protective measures, and comparing the cost of the approaches.

Steps in the Process

The first step is to list assets. CAPTool includes a complete list of assets—for example, bridges and tunnels, transit and rail stations, administration and support facilities, ferries and fleets—and allows the user to add others.

The second step is to evaluate hazards and threats. CAPTA divides threats into two categories—unintentional hazards and intentional threats. Unintentional hazards include major power outages, structural failures, and devastation or massive disruption from natural hazards such as floods, earthquakes, and extreme weather. Intentional threats involve deliberate attempts to disrupt a system, as happened to public transit in London, England, and to the rail service in Madrid, Spain.

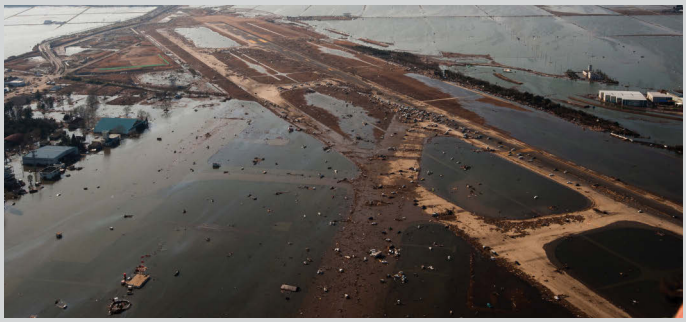


PHOTO: SAMUEL MORSE, U.S. AIR FORCE

The recent earthquake and tsunami in Sendai, Japan, caused much destruction, including flooding of the Sendai Airport. NCHRP Report 525, Volume 15, provides guidance on evaluating threats—both intentional and unintentional—to transportation assets.

Every agency may have to deal with a terrorist attack, although the severity of the risk will have to be assessed with information from law enforcement. Some agencies also have to deal with the hazards of flood plains, tornadoes, or earthquakes. CAPTool allows the selection of hazards and threats of concern; users can add specific local hazards and threats.

Step three is to evaluate the potential impact of an event by identifying what is critical for operation. What can an agency least afford to lose? What losses can it cope with? CAPTA assists in identifying critical assets and assessing the consequences of their loss. For example, if a bridge went down, from whatever

columns benefit from wraparound pressures, once the shock flow engulfs the column. The bridge column disrupts the shock flow, causing highly turbulent behavior behind the column. Positive pressures were shown to act along the back of the bridge column, partly negating the reflected pressures acting along the column's front.

Other Tests

Researchers at SUNY Buffalo conducted a similar computational study of the behavior of shock waves near structural steel wide flange sections (*15*). The results agreed with the findings from the NCHRP project. In particular, a 50 percent nominal decrease was reported in the net reflected impulse because of the enhanced clearing and wraparound pressure effects.

State-of-the-art computational tools are being applied to other complex problems associated with bulk explosive threats against highway bridges. For instance, the effects of an above-deck detonation on the performance of cable-stayed and suspension bridge decks was investigated at the University of California, Berkeley (*16*), and the U.S. Army Engineer Research and Development Center conducted a companion computational study to the experimental blast testing of structural steel suspension bridge towers (*12*).

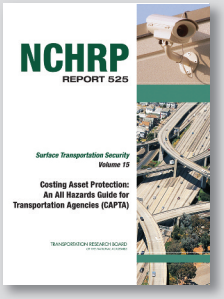
Tools, Provisions, Techniques

The experimental and computational research efforts have provided sufficient information to begin development of bridge-specific engineering tools, protective design provisions, and retrofit techniques that

cause, what would that do to a bus company? If a ferry sank, how would the company carry on? How many people would be put at risk by the loss of a specific asset?

Step four addresses countermeasures to protect assets, including a range of activities from prediction to detection to deterrence to response. The guide lists alternatives—such as security cameras or dog patrols, improved fencing, or a new pass system to control access to facilities—but the user makes the choices. CAPTool helps indicate the costs of the choices, but because costs vary across the country, only rough estimates can be provided; the user would have to determine the actual costs. Once again, users can add protective measures to the CAPTool list.

The last step is to decide which countermeasures are appropriate and affordable. CAPTool helps determine the costs of various mixes of alternatives to identify the approaches that can maximize what the agency can do within its resources.



Focus on Consequences

CAPTool and its user guide are available by download; the program runs in two versions: a basic version for smaller agencies and an enhanced version for agencies with a range of assets. But all agencies have to make the same decisions, and the basic CAPTool is a good starting point for all users—CAPTool requires familiarity with Microsoft Excel; moreover, after examining the initial results, an agency may opt for additional run-throughs to reassess the initial results. Making the run-throughs on the basic CAPTool can increase a user's comfort when moving to the enhanced version.

The guide and CAPTool are not classified—they only raise questions and list options. Although covering sensitive issues, CAPTool does not include sensitive data—until it is used. As soon as an agency has entered data about its own situation and indicated its choices, however, anyone could find out the vulnerabilities—information that an agency would want to secure.

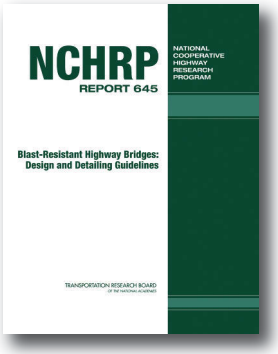
The CAPTA guide is consequence-driven, allowing a user to examine the cost of various approaches to asset protection and to understand the possible consequences. Each user must decide not only whether an asset might be lost or service disrupted but the seriousness of the consequences. With the CAPTA guidance, agency users can make rational decisions based on their own assessment of assets, their own assessment of the threats to those assets, their own decisions about the most critical assets, and their knowledge of available funding.

An agency can reuse CAPTool to enter data about new assets, adjust judgments about hazards and threats and what is critical, and revise options from new information, new intelligence, and financial resources. The guide and software function as living tools.

The panel that oversaw the design of the CAPTA guide and CAPTool focused at first on new threats—on possible terrorist attacks. The members of the panel then realized that the source of the threat was only one issue—the loss of an asset has the same consequence whatever the cause of the loss. The guide and software, therefore, are designed to cover all possible hazards and threats.

NCHRP Report 525, Volume 15, *Costing Asset Protection: An All-Hazards Guide for Transportation Agencies (CAPTA)*, 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 is Professor Emeritus and Director, Emergency Communications Research Unit, Carleton University, Ottawa, Ontario, Canada. He was a member of the National Cooperative Highway Research Program (NCHRP) project panel that oversaw the preparation of NCHRP Report 525, Volume 15, Costing Asset Protection: An All-Hazards Guide for Transportation Agencies (CAPTA).



For more information about NCHRP Report 645, Blast-Resistant Highway Bridges: Design and Detailing Guidelines*, go to www.TRB.org/SecurityPubs/.*

can mitigate a blast threat. The U.S. Army Engineer Research and Development Center has devised bridge-specific software to characterize blast loads, Bridge Explosive Loading (BEL), which combines the capabilities of CONWEP and BlastX, providing a versatile engineering tool for predicting blast loads on highway bridge components.

Although BEL is not yet able to account for reduced blast loads on slender structural components, the results from the NCHRP-funded bridge column research are being applied to add this capability. The NCHRP results also have assisted in the development of blast-resistant design provisions for highway bridge columns (*9*). The proposed provisions classify bridge columns into three categories based on the scaled standoff of the bulk explosive threat, a common parameter in guidelines for blast-resistant design.

In general, the severity of blast effects on highway bridge columns increases as the standoff decreases. Accordingly, the proposed blast-resistant design provisions become increasingly stringent as the scaled standoff decreases. More detailed information is available in NCHRP Report 645 (*9*).

Computational research from the University of California, Berkeley, on the effects of above-deck detonations on cable-stayed and suspension bridge decks (*16*) led to the concept of a frangible deck panel designed to fail early and to vent loads that the structure otherwise would resist. Frangible deck panels can be installed near the bridge towers; if a bridge tower is attacked with an above-deck detonation, the frangible deck panels will absorb blast energy via disintegration, so that pressure venting occurs, decreasing the blast effects and protecting the structural integrity of the bridge tower.

Fortifying Infrastructure

Terrorist attacks on public transportation infrastructure have increased worldwide in recent years, raising concerns about the vulnerability of U.S. highway bridges. Despite this trend, provisions for blast-resistant design have not been part of major U.S. bridge design specifications. America's transportation infrastructure therefore needs to be fortified through appropriate planning, and necessary protective measures need to be implemented through prioritized funding.

An initial research focus has been on highway bridge columns, which are critical to the structural integrity of a typical highway bridge and may be susceptible to terrorist threats. Research has commenced on other critical bridge components, to increase the U.S. transportation system's level of preparedness for potential terrorist attacks on major transportation corridors.

References

1. Jenkins, B. M., and B. R. Butterworth. *Explosives and Incendiaries Used in Terrorist Attacks on Public Surface Transportation: A Preliminary Empirical Examination*. Report WP 09-02, Mineta Transportation Institute, San Jose State University College of Business, San Jose, California, 2010.
2. Jenkins, B. M. *Protecting Surface Transportation Systems and Patrons from Terrorist Activities: Case Studies of Best Security Practices and a Chronology of Attacks*. Report 97-04, Mineta Transportation Institute, San Jose State University College of Business, San Jose, California, 1997.
3. Blue Ribbon Panel on Bridge and Tunnel Security. *Recommendations for Bridge and Tunnel Security*. American Association of State Highway and Transportation Officials and Federal Highway Administration, Washington, D.C., 2003.
4. *National Response Team Incident Summaries*. www.nrc.uscg.mil/insum2004/bombthreat.html.
5. Jenkins, B. M., and L. N. Gersten. *Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices*. Report 01-07, Mineta Transportation Institute, San Jose State University College of Business, San Jose, California, 2001.
6. Winget, D. G., K. A. Marchand, and E. B. Williamson. Analysis and Design of Critical Bridges Subjected to Blast Loads. *Journal of Structural Engineering*, Vol. 131, No. 8, pp. 1243–1255, 2005.
7. Science Applications International Corporation. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*. American Association of State Highway and Transportation Officials, Washington, D.C., 2002.
8. Ray, J. C. Risk-Based Prioritization of Terrorist Threat Mitigation Measures on Bridges. *Journal of Bridge Engineering*, Vol. 12, No. 2, pp. 140–146, 2007.
9. Williamson, E. B., O. Bayrak, G. D. Williams, C. E. Davis, K. A. Marchand, A. E. McKay, J. Kulicki, and W. Wassef. *NCHRP Report 645: Blast-Resistant Highway Bridges: Design and Detailing Guidelines*. Transportation Research Board of the National Academies, Washington, D.C., 2010.
10. Fujikura, S., and M. Bruneau. *Experimental and Analytical Investigation of Blast Performance of Seismically Resistant Bridge Piers*. MCEER-08-0028, Multidisciplinary Center for Earthquake Engineering Research, Buffalo, N.Y., 2008.
11. Cofer, W. F., D. S. Matthews, and D. I. McLean. Effects of Blast Loading on Prestressed Girder Bridges. In *Proceedings of the 80th Shock and Vibration Symposium*, San Diego, California, 2009.
12. Ray, J. C. Validation of Numerical Modeling and Analysis of Steel Bridge Towers Subjected to Blast Loadings. In *Proceedings of 2006 Structures Congress*, American Society of Civil Engineers, 2006.
13. Ray, J. C., B. J. Armstrong, and T. R. Slawson. Airblast Environment Beneath a Bridge Overpass. In *Transportation Research Record: Journal of the Transportation Research Board, No. 1827*, Transportation Research Board of the National Academies, Washington, D.C., pp. 63–68, 2003.
14. Williams, G. D. Analysis and Response Mechanisms of Blast-Loaded Reinforced Concrete Columns. PhD dissertation. University of Texas at Austin, May 2009.
15. Ballantyne, G. J., A. S. Whittaker, G. F. Dargush, and A. J. Aref. Air-Blast Effects on Structural Shapes of Finite Width. *Journal of Structural Engineering*, Vol. 136, No. 2, pp. 152–159, 2010.
16. Son, J., and A. Astaneh-Asl. Blast Protection of Cable-Stayed and Suspension Bridges. In *Proceedings of the Technical Council on Lifeline Earthquake Engineering Conference*, American Society of Civil Engineers, 2009.

Planning for Bridge Security

STEVE ERNST

Incorporating security early in project development can enhance structural resilience significantly by increasing the standoff from critical components and by restricting or eliminating access for threats. The highway funding legislation of 2005—the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users—identified security as a separate item and required that metropolitan and statewide planning processes "increase the security of the transportation system for motorized and nonmotorized users."

Carrying out this requirement often is possible only if measures are considered in the environmental process or at the real estate acquisition phase of a project. Security measures may include establishing room for standoff at a bridge site, installing standpipes for firefighting, or placing cameras and lighting to improve detection and response. An early look at security is also cost-efficient, because features incorporated during planning can be much less expensive than protective measures added later.

PHOTO: WIKIMEDIA COMMONS

The I-40 Bridge near Oklahoma City failed when a barge, out of the channel and traveling upstream, struck and damaged a bridge column, causing the span to drop.

For example, a pier in a navigable waterway can be protected from intentional acts of terrorism and from unintentional barge collision by placement of rock islands, dolphins—that is, man-made structures above the water level but not connected to the shore—or protective fenders. The rock island option may be the best security against intentional ramming and explosions. This option, however, requires environmental studies of the footprint's impact on the waterway; adding the feature after the original clearances requires expenditures of time and money.

The Federal Highway Administration (FHWA) promotes a managed-risk approach for bridge security, derived from the methodology developed by Ray (*1*). The process evaluates the benefits from security measures for bridge components as a function of three elements:

- The importance of the component to the bridge's stability;
- The vulnerability of the component to a possible threat; and
- Measures for the likelihood that the threat will occur.

PHOTO: WIKIMEDIA COMMONS

Dolphin barriers.

Because the threat of terrorism to any particular bridge is unknown, the approach focuses on developing a list of reasonable security projects, based on cost and on the relative merit as determined through the quantitative analysis. Bridge owners and operators can consider potential security projects along with projects to protect against other hazards or to ensure long-term performance. Although the quantitative analysis can assist in developing a list of security projects, bridge owners and operators also should weigh their own experience and apply their own expert judgment in deciding how best to address security.

The author is Structural Engineer, Federal Highway Administration, Washington, D.C.

A rock island was included in the construction plans of a major bridge to protect the pier from ship collision and acts of terrorism.

Reference

1. Ray, J. C. Risk-Based Prioritization of Terrorist Threat Mitigation Measures on Bridges. *Journal of Bridge Engineering*, Vol. 12, No. 2, pp. 140–146, 2007.

SECURITY & CRITICAL INFRASTRUCTURE PROTECTION

PHOTO: LARRY LEVINE, WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

Addressing Vulnerabilities in Transit Security

Developments Since September 11, 2001

YUKO J. NAKANISHI

The author is Principal, Nakanishi Research and Consulting, LLC, Rego Park, New York, and Chair of the TRB Critical Transportation Infrastructure Protection Committee.

Above: Public transportation hubs, such as the Suitland Metro station in metropolitan Washington, D.C., comprise many forms of transit—pedestrian, bicycle, rail, automobile, and bus—and can be vulnerable to security threats.

Public transportation provided more than 10.4 billion trips in the United States in 2009, totaling 55.2 billion miles traveled. Transit is vital to the nation's economy and to its residents. Commuters depend on transit to get to their jobs, and retailers depend on transit to get customers to their shops. For some residents, transit is a lifeline service, the only mode of transportation available. Without transit, traffic congestion would worsen, especially in metropolitan areas, and prevent the on-time delivery of goods.

Major disruptions to transit systems, therefore, whether through terrorism, natural disasters, accidents, or other causes, can inflict economic harm on a metropolitan region. For example, the interruption of service during he three-day strike by New York City transit workers in December 2005 demonstrated the importance of the transit system to the city and its economy—many residents had difficulty getting to their jobs or could not get to work at all. The loss of the system could cost the city and its employers hundreds of millions of dollars daily in lost productivity, lost sales, and lost tax revenues.

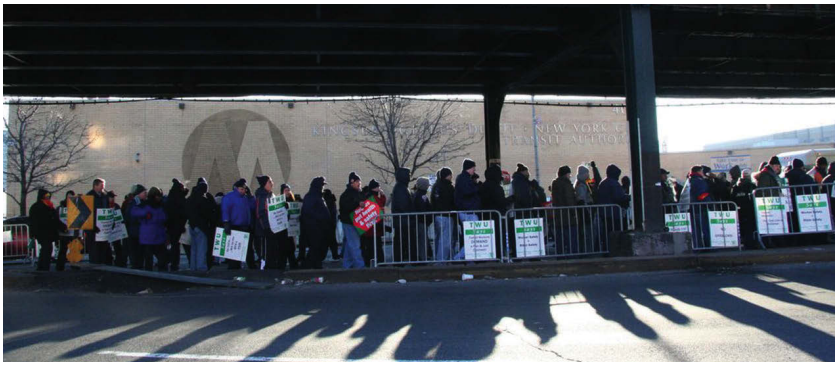


PHOTO: SANDER KOYFMAN

The 2005 strike by New York City transit workers demonstrated the value of the transit system to the city's daily life and economy.

The September 11, 2001 (9/11), attacks on the World Trade Center (WTC) were not directed at the transit system, but the system sustained collateral damage—track was destroyed, and the Port Authority Trans-Hudson (PATH) WTC train station and several New York City Transit stations nearby had to be shut down for repairs. Ridership decreased during the weeks after the attacks.

Because the stations were hit at the terminals of routes, however, trains could be rerouted. A direct and extensive attack on the New York City transit system could have devastating economic consequences. In addition to physical trauma and economic

loss, acts of terrorism cause psychological trauma, including short- and long-term anxiety, posttraumatic stress disorder, and other stress-related problems, as evidenced in 9/11 survivors and area residents.

Transit's Vulnerability

Transit is vulnerable because of its vast infrastructure, the congregation of people within enclosed spaces, and its ease of access. Terrorists may target not only the vehicles and the people aboard, but also the critical infrastructure and buildings nearby, or they may use the vehicles as conduits for chemical or biological weapons—the ventilation systems of heavy rail, for example, could disseminate airborne threats quickly.

Transit systems rely on extensive communications and control networks, and the likelihood that transit assets could be harmed through these networks looms larger as computer hackers increase in sophistication and nation-states gain expertise in cyberwarfare. In selecting and implementing security measures, agencies must consider customer service and operational effects, the issues of privacy and constitutionality that may arise in implementation, and the perspectives of employees and passengers.

Worldwide, 684 attacks have targeted buses since 1970—mostly scheduled buses, as well as bus stations; improvised explosive devices (IEDs) were used in 50 percent of the attacks and automatic weapons in another 16 percent. Of the 354 train attacks worldwide, more than 55 percent targeted passenger intercity or commuter trains, and 28 percent targeted train stations. Of the attacks on passenger rail, 79 percent involved IEDs or other explosives (*1*).

In particular, attacks on commuter rail systems have claimed many innocent lives. In Madrid, Spain, in 2004, almost 200 commuter rail passengers were killed and hundreds more injured, and in Mumbai, India, in 2006, commuter rail attacks killed 200 persons and injured many more. In Russia, passenger trains have been attacked and derailed by terrorists; a 2009 bombing of a luxury train killed 25 and injured almost 100. The London subway and bus systems attacks in 2005 killed more than 50 persons.

These attacks are successes from the viewpoint of the terrorists and therefore are highly likely to continue, targeting transit systems around the world as well as in the United States. Al-Qaeda terrorists are "lethal and destructive" and seek targets that "promise the highest body counts" (2, p. 54).

In 2006, terrorists planned to plant explosives on a PATH train to destroy the underwater tunnel connecting Manhattan and New Jersey and kill hundreds of commuters. In 2009, the Christmas Day underwear bomber attempted to bring down a plane destined for Detroit, Michigan. Also in 2009, Al-Qaeda planned suicide bomber attacks on New York City's subway system.

PHOTO: FRANCIS TYERS

London's Russell Square after bombings of the city's subway and bus system in 2005. Attacks on transit and commuter rail systems can be particularly deadly—the London bombings killed more than 50 people.

Immediately after 9/11, the United States reorganized and strengthened the intelligence community by establishing the Transportation Security Administration (TSA) and the Department of Homeland Security (DHS) through the Aviation and Transportation Security Act and the Homeland Security Act of 2002. TSA, now housed within DHS, exercises federal responsibility for transit security; the Federal Transit Administration (FTA) provides key support on security matters to transit agencies through training, research, technical assistance, demonstration projects, and grants.

FTA requires agencies to spend at least 1 percent of their Urbanized Area Formula Program (Section 5307) funds on security projects and has expanded the definition of capital programs to include security training, exercises, and planning. In addition, FTA requires that fixed guideway rail systems maintain a system security plan. The Federal Railroad Administration is the primary rail safety regulatory authority for commuter rail operators and Amtrak and ensures the implementation of safety and emergency preparedness plans.

Federal Vision for Transit Security

TSA participates in a unified national effort to protect and secure the nation's intermodal transportation systems. The goal is to build a resilient, robust, and sustainable network of federal, state, and local governments, law enforcement, emergency response, and private-sector partners, ensuring the safe movement of passengers and promoting the free flow of commerce.

Photo: Larry Levine, WMATA

Blue Tide, or Terrorism Identification and Deterrence Effort, is a joint police operation for Washington, D.C.–area rail transit station safety involving the WMATA Metro Transit Police Department, Transportation Security Administration VIPR teams, and local police.

TSA's vision for mass transit and passenger rail is "a secure, resilient transit system that leverages public awareness, technology, and layered security programs while maintaining the efficient flow of passengers and encouraging the expanded use of the nation's transit services" (*3*). This vision emphasizes that security must be provided without impeding customer service and public access to transit services.

Although no threats appear imminent, randomly deployed and layered security measures can be seen at any time in rail and transit stations and at airports throughout the country to strengthen security efforts and keep Americans safe. TSA is raising the baseline for mass transit security through unpredictable, visible deterrents; research and development; and expanded connectivity with state and local entities. The focus is on greater information sharing, increased training and public awareness, and greater assistance and funding for rail transit activities. Security-related grants and awards to rail systems around the country total millions of dollars each year.

Partnerships between TSA and local authorities support mass transit security not only through grants, but with comprehensive security inspections, deployment of canine teams for explosives detection, and frequent but unpredictable deployment of Visible Intermodal Prevention and Response (VIPR) teams to mitigate evolving threats and enhance security for the traveling public.

Protective Measures and Practices

Protective measures and practices implemented in the past decade include risk assessments, as well as assessments of threat and vulnerability; new or improved security and emergency preparedness plans; security training for frontline workers and specialized counterterrorism training for transit police and security; "eyes and ears" public outreach initiatives; video surveillance and other technologies; VIPR teams; canine teams, and other protective measures (*4*). Transit agencies also have become more involved in regional interagency efforts and have participated in larger-scale drills and exercises.

Many agencies have applied for and received federal funds through TSA's Transit Security Grant Program, which allocates resources through a flexible process focused on reducing risks. Measures that address typical crime such as assaults on bus operators also can help in counterterrorism efforts. The Transportation Research Board's (TRB) Transit Cooperative Research Program (TCRP) has assembled state-of-the-practice information about protective measures, published in TCRP Synthesis 80, *Transit Security Update*[1] (2009), and in a forthcoming TCRP Synthesis on *Practices to Protect Bus Operators from Passenger Assault*.[2]

Following are some of the protective measures in use by transit agencies.

Risk and Security Assessments

Risk and security assessments assist TSA, FTA, and transit agencies in developing security profiles and establishing baselines; understanding strengths and vulnerabilities; and measuring security improvements. The assessments also assist in allocating transit security funds.

TSA has examined threat, vulnerability, and consequences for more than 200 mass transit and passenger rail scenarios through the Transportation Systems Sector Risk Assessment and has conducted inspections and provided technical assistance through the Surface Transportation Security Inspection Program. Through TSA's Baseline Assessment for Security Enhancement program, inspectors are monitoring progress on the 17 security and emergency management action items developed with FTA. Several security risk and vulnerability tools are being combined into a comprehensive platform.

Information and Intelligence Sharing

Information and intelligence sharing involves regional coordination and interagency committees and task forces, the development of web-based resources, and participation in conferences and workshops. Federal agencies share intelligence with transit security directors and law enforcement in selected metropolitan areas through the Joint Terrorism Task Force (JTTF). TSA also disseminates mass transit security awareness messages to transit

[1] http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_syn_80.pdf.
[2] TCRP Synthesis J-07: Synthesis of Information Related to Transit Problems, Topic SF-14.

operators; the Transportation Security–Information Sharing and Analysis Center website assists agencies in working together to understand threats; develop solutions to technical, implementation, and operational issues; and share lessons learned.

Individual agencies also facilitate information sharing between and among transit police or security officers, law enforcement, and workers, as well as the community; this effort is useful in identifying unusual activity, monitoring transit operations by terrorists or criminals, and increasing the awareness of transit employees about specific threats and crimes. TSA supports these initiatives through the Intermodal Security Training and Exercise Program, or I-STEP, and the Bomb Squad Response to Transportation Systems–Mass Transit program.

Information sharing also takes place through the joint TSA and FTA Connecting Communities effort, a forum for federal transportation security partners to interact with state and local governments and local responders. TSA, FTA, and the Federal Emergency Management Agency (FEMA) conduct roundtables for the security and safety directors of the 50 largest mass transit and passenger rail agencies to meet with government and industry leaders, police, and other officials.

TSA also has deployed secure telephones at selected transit agencies and Amtrak, and implemented a Private Industry Security Clearance Program to facilitate the sharing of sensitive or classified information. The dissemination of research results from TCRP projects electronically and through workshops and conferences also advances the goal of information sharing.

Passenger Security Inspections

Passenger security inspections (PSIs) involve random baggage inspections, canine patrols, and behavioral assessment of transit passengers without grounds of suspicion. Bag inspections are random and are conducted manually or with the assistance of portable trace detectors. The Massachusetts Bay Transportation Authority (MBTA) in metropolitan Boston, New York's Metropolitan Transportation Authority (MTA), WMATA, and New Jersey's NJ Transit have implemented random inspections.

Transit agencies are deploying canine patrols to detect explosives; the patrols offer mobility and rapid deployment. TSA has a canine certification program and offers specialized training for canine teams. As of December 2009, 15 transit systems have deployed 82 TSA-certified explosives-detecting canine teams.

Transit personnel can be trained in behavioral assessment—the only PSI procedure not restricted to police. The training heightens observational skills for identifying suspicious persons and activities. A few transit agencies, including MBTA and some ferry operators, have trained their police or personnel in behavioral assessment.

PSIs have legal and constitutional implications, however. TCRP Report 86, Volume 13, *Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers*, reviews the merits of PSIs and the legal, institutional, operational, technical, and other issues—as well as customer and employee perspectives—that agencies need to consider before implementation; the guide helps agencies determine whether to use PSIs, which ones to use, and how to implement a program (5).

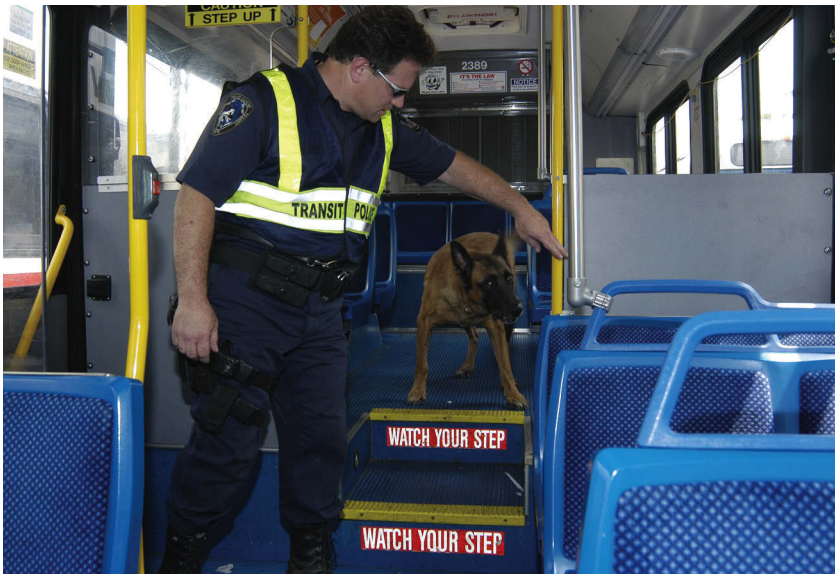
Transit Security Grant Program

TSA reviews and prioritizes projects for the Transit Security Grant Program; final awards are decided with input from DHS and FEMA. Project proposals are assessed for addressing all three elements of risk—threat, vulnerability, and consequence—with particular attention to variations in vulnerability.

TSA works with local entities and FEMA to determine the most significant vulnerabilities and consequences of a transit system attack and provides funding for projects that best enhance security. The grant program strives to remain flexible and transparent in providing risk-based funding to cities and states that face the greatest threat, while ensuring a fundamental level of protection across the country.

Transit grants enhance the security of critical infrastructure and provide for employee training, antiterrorism exercises, and public awareness campaigns. Grants also fund specially trained antiterrorism law enforcement teams and technologies to enhance detection.

PHOTO: LARRY LEVINE, WMATA



Transit systems such as WMATA in Washington, D.C., often deploy canine patrols to detect explosives.

Be Alert templates from Transit Watch.

Transit Watch and Security Awareness

Transit police or security cannot be in all places at all times—security force multipliers are essential. Educating transit workers, passengers, and the public—including area vendors—about security awareness and issuing continuous reminders about being alert and reporting suspicious activity are helpful initiatives for expanding the reach of police and security.

FTA initiated the Transit Watch program in 2003 and added enhancements working with TSA in 2006. Transit Watch assists transit agencies with public and employee outreach by providing toolkits that can be adapted to the systems. Examples of Transit Watch templates are shown above. The program aims to raise the awareness of passengers and transit workers about suspicious activity or items and to educate passengers about how to evacuate the system safely.

DHS and TSA recently partnered with several transportation entities, including New York's MTA, Amtrak, and the Washington [D.C.] Metropolitan Area Transit Authority (WMATA), to promote the campaign, "If You See Something, Say Something," encouraging the public to report suspicious activity. TSA Administrator John S. Pistole noted, "As we saw in the Times Square attempted bombing, the public plays a key role in security" (*6*). The partnerships have increased awareness and security throughout the nation's transportation systems.

National Tunnel Security Initiative

A Tunnel Risk Mitigation Working Group, with representatives from DHS, FEMA, FTA, and JTTF, is working on reducing the risk of breaches in underwater mass transit tunnels.

Technologies

Technologies such as video surveillance and automated vehicle location (AVL) systems serve multiple purposes and can give responders important situational awareness about an incident or emergency; other technologies, such as radiological pagers and portable trace explosives detectors, have an exclusive counterterrorism focus (*4*). Key technologies in use by transit agencies to enhance system security are described below.

◆ *Video surveillance*, implemented by a majority of transit agencies on vehicles and in stations and terminals, requires significant capital investment but is considered cost-effective because the systems are versatile. As an agency's security budget increases, cameras can be added to the fleet; moreover, analog systems can be upgraded to digital, wireless systems.

Video can be used for counterterrorism, accident investigations, identification of criminals, worker compensation cases, and resolution of customer complaints. Combined with threat detection systems, video can allow responders to view a threat in real time.

(continued on page 26)

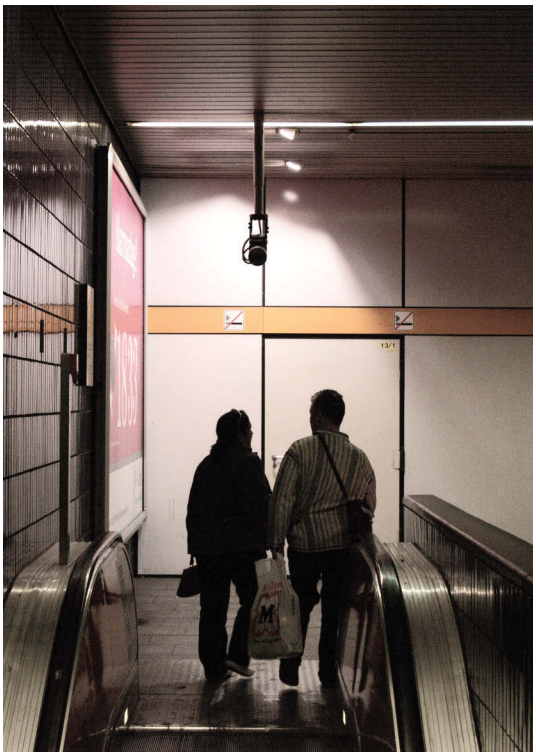


PHOTO: KARL MOOR

Despite the large initial expense, video surveillance systems are versatile and are considered a cost-effective technology for transit agencies.

Trust Builds Speed

Communicating Emergency Transportation Options to Vulnerable Populations

DEBORAH MATHERLY AND JANE MOBLEY

Studies of plans for emergency response operations make clear that communication is critical to help people who are vulnerable to understand their transportation options and the role of transportation agencies in providing those options. Inclusive communication by transportation agencies with these populations, however, is generally lacking.

To address this gap, the Transportation Research Board's Transit Cooperative Research Program (TCRP) has published *Communication with Vulnerable Populations: A Transportation and Emergency Management Toolkit* (TCRP Report 150). The toolkit demonstrates how transportation agencies can develop a process to communicate with vulnerable populations about transportation options during emergencies.

The toolkit provides a framework and tools for constructing a scalable, adaptable communication process that involves a network of agencies from the public, private, and nonprofit sectors. Through collaboration and partnering, these agencies can establish interconnected channels to deliver emergency communication in far-reaching and resourceful ways.

At the 2008 conference of the National Public Health Information Coalition, Lieutenant General (Ret.) Russel L. Honoré reminded participants that "trust builds speed." The principle applies not only to emergency planning and response but to the interactions of the public, volunteer, and private sectors. The more trustworthy the messenger and the message, the more likely people will listen and respond. Building the type of communication network described in the toolkit creates trustworthy working relationships that in turn support preparedness planning and swift responses.

The report describes the steps for network building:

1. Gather information:
   - Identify the vulnerable populations to be reached with emergency information and
   - Assess the need and capacity to communicate with them about transportation;
2. Build a network of public-sector agencies and community, volunteer, and private-sector organizations;
3. Communicate through the network; and
4. Sustain the network through agreements and performance measurement.

The approach dramatically expands the outreach capacity to vulnerable populations, shares the responsibility for the outreach, and requires inclusive planning by government agencies, nongovernmental organizations, and the private sector.

Public agencies have tested and implemented this approach successfully in the field. A communications network established by the Kentucky Cabinet for Health and Family Services, for example, was recognized for pandemic planning by the Center for Infectious Disease Research and Policy and is used by the U.S. Centers for Disease Control and Prevention in federal guidance as a model for national health organizations.

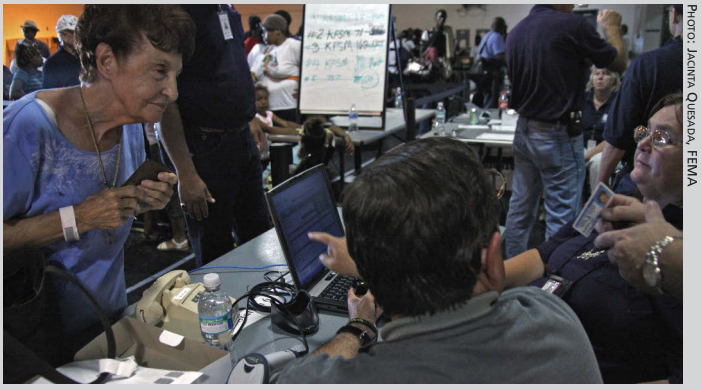


PHOTO: JACINTA QUESADA, FEMA

Evacuation procedures during Hurricane Gustav in New Orleans, Louisiana, in 2008. Transit Cooperative Research Program Report 150 outlines steps for communicating emergency transportation options to the elderly and other vulnerable populations.

According to the process outlined in the toolkit,

- The collaborative process at the local level can start with one person, a champion, who responds to the call to action and begins the work. The toolkit is designed to help a champion get started and bring others into the process.
- Emergency management is primarily responsible for communication in emergencies but may delegate the outreach to agencies already interacting with vulnerable populations. In some communities, transportation, public health, or other agencies may take the lead in the collaborative communication network for vulnerable populations.
- The agencies and organizations that participate in the network may vary from locality to locality.
- Communities differ in approaches to collaboration. Even communities with established, active partnerships, however, can evaluate practices and look for new opportunities to ensure that vulnerable populations can receive and act on critical messages.

The inclusive communication process described in the toolkit aims to inform vulnerable populations about emergency transportation options with actionable, easy-to-understand messages delivered through a network built on trusted relationships.

TCRP Report 150, *Communication with Vulnerable Populations: A Transportation and Emergency Management Toolkit*, 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.

Matherly is Principal Planner, Louis Berger Group, Inc., Washington, D.C. Mobley is Founding Principal, Jane Mobley Associates, Kansas City, Missouri.

Addressing Vulnerabilities in Transit Security
(continued from page 24)

Intelligent video uses video analytics to alert the dispatcher or law enforcement personnel automatically about real-time threats—for example, to unauthorized persons entering a transit facility or to abandoned packages on the premises. Intelligent video also tracks the movement of the threat or intruder. Although not yet in wide use, intelligent video can greatly enhance the surveillance capabilities of transit police and security personnel.

- *Automated vehicle location*—AVL systems track the location of transit vehicles and facilitate fleet management. In emergencies, the systems can alert dispatchers automatically if a transit vehicle goes off route. In addition, AVL can decrease emergency response times.
- *Radiological pagers* detect nuclear threats in transit systems.
- *Explosives trace detection technology* is available in portable devices, ideal for PSIs and for the rapid assessment of abandoned or suspicious objects.
- *Other threat detection technologies* are undergoing testing and implementation.
- *Emergency communications, head signs, and panic buttons*—Transit vehicles are usually equipped with emergency communications mechanisms that allow the operator one-way communications with a dispatcher. Electronic head signs activated by a panic button may display a message, such as "Call 911," to alert the public that the vehicle operator is in distress. Panic buttons also can alert the control center about an emergency incident. These technologies are important in the case of a hijacking or an assault.

TSA is working with DHS and the mass transit and passenger rail industry to identify technology needs and possible solutions and to coordinate research and development. TSA and key stakeholders will pilot-test security technologies at transit agencies.

Identity Management

Identity management is important in preventing unauthorized persons from entering or accessing secure areas or equipment. Transit agencies have applied identity management in conjunction with access and perimeter controls and in background screenings before hiring.

Security Training

Most transit agencies have implemented security awareness training for their frontline workers. Other available training includes emergency response, prevention and mitigation of IEDs and weapons of mass destruction, transit vehicle hijacking prevention and response, and recognition of suspicious behavior. FTA has developed security-related training courses and content through the National Transit Institute (NTI), the Transportation Safety Institute, and Johns Hopkins University (*4*). TSA recently created a Mass Transit Security Training Program to enhance training quality and consistency.

An FTA publication, *Immediate Actions for Transit Agencies*, assists transit workers who encounter life-threatening situations.[3] Working with NTI, FTA has developed and widely distributed guides on system security for transit employees. A training video, *The Mark*, was created in 2007 to demonstrate to transit employees the importance of being alert and asking the right questions; the video is available on FTA's safety and security website.[4] Another video, *System Security Awareness for Transit Employees: Warning Signs*, was created in 2003 and helps employees understand what to look for and what to do when confronted with suspicious activity, packages, devices, or substances.[4]

Police and Security Personnel

Police and security forces have expanded to include counterterrorism positions and activities. Counterterrorism measures initiated since 9/11 include high-visibility patrols, PSIs, and security sweeps of trains, stations, terminals, and buses.

VIPR Teams

TSA deploys VIPR teams in coordination with local law enforcement partners to keep transportation systems safe and secure. VIPR teams comprise federal, state, and local law enforcement officers, including some trained in behavioral observation and in security assets, such as canine teams. The goal is to help TSA leverage resources quickly to increase security in mass transit, passenger rail, and all other transportation modes anywhere in the United States.

The VIPR teams are intended to provide a deterrent force that is capable, visible, and adaptable, supplementing security resources and providing a deterrent presence. The teams can be deployed as needed to work with state and local security and law enforcement officials; rapid deployment is key. VIPRs provide detection and response capabilities and expand the range of security measures to detect, deter, or disrupt potential criminal or terrorist operations during heightened alerts or in the aftermath of an incident.

(continued on page 28)

[3] http://transit-safety.fta.dot.gov/security/SecurityInitiatives/ImmediateActions/HTML/IAs.html.
[4] http://transit-safety.volpe.dot.gov/security/TrainingTools/default.asp.

All-Hazards Planning

Coordinating the Many Levels of Emergency Response

CHARLES E. WALLACE

In response to the destructive effects of September 11, 2001, Hurricane Katrina, and other setbacks, the United States has improved planning for responses to incidents of all types and severity—or all-hazards threats. Initiatives include the consolidation of federal emergency management and security agencies into the new Department of Homeland Security (DHS); the release of presidential directives, policies, and guidelines; and the development of a systematic set of doctrines and procedures for emergency preparedness and response.

The owner-operators of surface transportation infrastructure—state, territorial, local, and tribal—are key players in the emergency response process. To assist them in this role, the National Cooperative Highway Research Program (NCHRP) has released *A Guide to Emergency Response Planning at State Transportation Agencies* (NCHRP Report 525, Volume 16). Following the basic structure of the Federal Emergency Management Agency's (FEMA) Comprehensive Preparedness Guide 101 (CPG 101), *Developing and Maintaining State, Territorial, Tribal, and Local Government Emergency Plans*, the NCHRP report integrates concepts from the National Incident Management System (NIMS) and the National Response Framework, incorporating recommendations from FEMA's 2005 review of all state Emergency Operations Plans (EOPs). The report addresses the target capabilities that are fundamental in implementing the National Preparedness Guidelines.

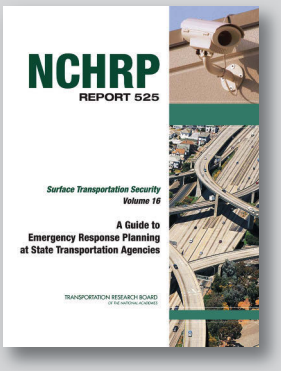
In addition to coverage of the institutional context for emergency response, the two major sections of the NCHRP report present

- Guidelines for developing an emergency response program—a detailed, step-by-step approach to assess the status of a transportation agency's planning for emergency response, relating emergency response planning and operations to emergency transportation operations; addressing ways to prioritize improvement for internal agency EOPs and the state EOP; introducing a high-level self-assessment tool; and identifying other external assessments; and
- Resources on surface transportation issues and emergency response policies and practices—offering additional guidance on organizational and staffing decisions and decision-making sequences, and providing an emergency response matrix and an action reference matrix, a detailed self-assessment tool to delineate goals and resources.

With workshops across the country, TRB's Second Strategic Highway Research Program is testing a proposed curriculum to establish core competencies for various first responder disciplines and to encourage cooperative, cross-discipline training.

The first section provides a detailed, high-level review, following the CPG 101 planning process—plan, prepare, respond, and recover—and targets emergency response planners and those who implement EOPs at state transportation agency central offices, regional or district offices, and transportation management centers. The NCHRP report also provides guidance for those involved in the design, deployment, operation, and maintenance of transportation infrastructure. The report includes extensive guidance based on NIMS and other national imperatives, as well as appendices with background and supporting materials.

NCHRP Report 525, Volume 16, *A Guide to Emergency Response Planning at State 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 is with Telvent Transportation–North America, Alachua, Florida.

Addressing Vulnerabilities in Transit Security
(continued from page 26)

Developing Resources

FTA has posted resources, including reports and publications, on its transit safety and security website.[5] The 2007 TSA-FTA report, *Security and Emergency Management Action Items for Transit Agencies,* addresses threats and risks, with an emphasis on closing gaps in security and emergency preparedness programs. *Transit Agency Security and Emergency Management Protective Measures,* produced in 2006 by FTA, in consultation with the TSA Office of Grants and Training and the American Public Transportation Association (APTA), presents a systems approach to implementing protective measures during an attack or incident and during the recovery. The 2004 report, *Transit Security Design Considerations,* details a range of security measures appropriate for transit systems, including strategies for crime prevention through environmental design.

APTA develops standards for public transportation security through committees and working groups on security standards policy and planning, cybersecurity, emergency management, infrastructure security, and security risk management. Published standards are posted on the APTA website.[6]

The Mineta Transportation Institute, a DHS National Transportation Security Center of Excellence, has assembled a database of all transportation-related terrorist incidents worldwide and has released several key publications on topics in public transportation and homeland security. Six other related DHS Centers of Excellence have produced relevant publications on "technologies, tools, and advanced methods to defend, protect and increase the resilience of the nation's multimodal transportation."

TRB's security and emergencies research website contains links to programs and activities[7]; another web page contains links to TRB publications on related topics.[8] Most notably, TCRP Synthesis 80, *Transit Security Update*, describes the practices and measures that transit agencies have implemented since 9/11 and presents five case studies: MBTA; San Francisco's Bay Area Rapid Transit; the Capital District Transportation Authority of Albany, New York; Capital Metro, Austin, Texas; and WMATA (*4*). Two appendices contain comprehensive supporting information and a literature review.

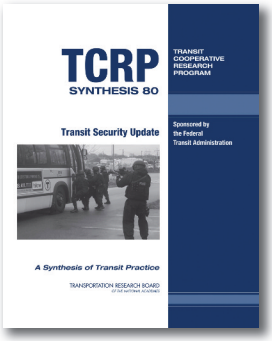
TCRP projects have focused on the communication of threats, customer communications and training, the use of canine units, robotic devices, portable devices for explosives detection, intrusion detection, passenger security inspections, security measures for ferry systems, tunnel security, hazard and security planning, guidelines for emergency training exercises, emergency mobilization and operations, and continuity-of-operations planning.

TRB's National Cooperative Highway Research Program (NCHRP) has published *Security 101: Physical Security Primer for Transportation Agencies*, Volume 14 of NCHRP Report 525, *Surface Transportation Security*, with sections specifically addressing transit security. Volume 15 of the series, *Costing Asset Protection: An All-Hazards Guide for Transportation Agencies (CAPTA),* assists multimodal agencies in making decisions about security investments.

Increasing Preparedness and Capabilities

Since 9/11, transit agencies have worked with TSA, FTA, and local partners on risk and vulnerability assessments, training and outreach, information sharing, surveillance and detection technologies, and the deployment of transit police, security personnel, and canine teams. As a result, transit systems have increased their preparedness and their capabilities to deter and detect terrorism.

The terror threat, however, continues to evolve, and terrorists will take advantage of any vulnerability to meet the objectives of destroying U.S. assets and killing American citizens. The transit industry therefore needs to remain vigilant, proactive, and agile to protect systems, passengers, employees, and the public.



Transit Cooperative Research Program Synthesis 80, *Transit Security Update*, presents case studies to illustrate measures and practices implemented since 9/11 by transit agencies across the country.

References

1. Jenkins, B. M., B. R. Butterworth, and K. S. Shrum. *Terrorist Attacks on Public Bus Transportation: A Preliminary Empirical Analysis*. Report 09-01, Mineta Transportation Institute, San Jose State University College of Business, San Jose, California, March 2010.
2. Jenkins, B. M., and B. R. Butterworth. *Potential Terrorist Uses of Highway-Borne Hazardous Materials*. Report 09-03, Mineta Transportation Institute, San Jose State University College of Business, San Jose, California, January 2010.
3. *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*. Transportation Security Administration, Department of Homeland Security, May 2007, p. A48.
4. Nakanishi, Y. J. *TCRP Synthesis 80: Transit Security Update*. Transportation Research Board of the National Academies, Washington, D.C., 2009.
5. Frazier, R., J. Waite, and Y. J. Nakanishi. *TCRP Report 86, Volume 13: Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers*. Transportation Research Board of the National Academies, Washington, D.C., 2007.
6. Transportation Security Administration. Press Release, July 26, 2010. www.tsa.gov/press/releases/2010/0726.shtm.

[5] http://transit-safety.volpe.dot.gov/.
[6] http:// aptastandards.com/Documents/PublishedStandards/Security/tabid/329/language/en-US/Default.aspx.
[7] TRB.org/SecurityEmergencies/SecurityandEmergencies1.aspx.
[8] TRB.org/SecurityPubs.

Improving Resilience in Rail Transit Corridors

Developing Models for Estimating the Impacts of System Disruptions

MICHAEL GREENBERG, KAREN LOWRIE, TAYFUR ALTIOK, MICHAEL LAHR, PAUL LIOY, AND HENRY MAYER

New Jersey Transit train at a station. The system is being used to model and test approaches to resilience after major disruptions.

The Northeast Corridor is the most heavily traveled in the United States and one of the most likely surface transportation targets for terrorists, considering the volume of passengers and the historical and political significance of the cities and sites along the route. The interoperable and connecting services make the major cities highly vulnerable. The Center for Transportation Safety, Security, and Risk (CTSSR) at Rutgers University is using the Northeast Corridor as a test bed to improve the resilience of passenger rail corridors; CTSSR is a National Transportation Security Center of Excellence (NTSCOE) of the U.S. Department of Homeland Security (DHS).

Three complementary simulation models in development at CTSSR will offer insights into events that can cause cascading impacts in rail and connected transportation systems, explore the consequences of those events, and identify investments that could increase system resilience after accidents and attacks. The models also will be valuable for education and training and for adaptation to other rail corridors.

Destructive cascading impacts begin when an event at one node or link disrupts transportation, and the disruption spreads beyond the immediate area. The impact from a serious rail passenger terrorist event, for example, may extend hundreds of miles along a corridor, spreading from the rail line to connecting light rail, bus, and highway networks.

Complementary Models

The first model in development, funded by DHS through NTSCOE, is an industrial systems model built with ARENA software. The model simulates the normal operation of a passenger rail corridor in the vicinity of a critical hub station and then perturbs it with natural or man-made events.

Working with planning and security personnel from NJ Transit, Amtrak, and the New Jersey Office of Homeland Security, the CTSSR team will examine how an event such as a bridge explosion would affect passenger flows and train movements along the rail lines and in the hub station. Output from the model will reveal points of backup and congestion under different scenarios and will suggest alternative routes or passenger flow plans that could build more resilience into the system. The model also could apply to the impacts of special sports or entertainment events, like the Super Bowl, on passenger movement and modal shifts.

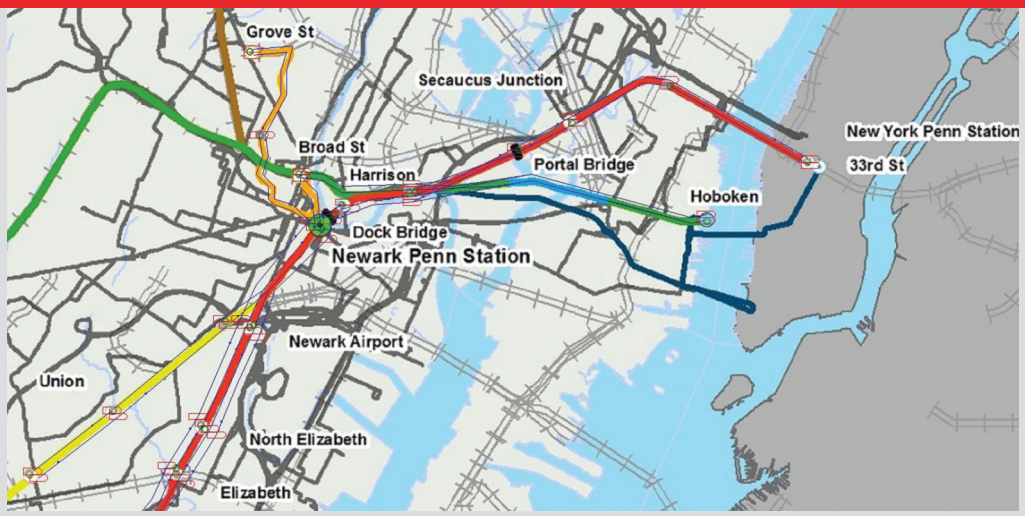
The second model, funded by the U.S. Department of Defense (DOD), examines the potential health impacts of a contaminant plume on passengers and workers at rail stations, other connecting transit systems, and on people in the area. Terrorists could create a plume, for example, by detonating explosives and radiological dispersion devices at a rail station or on an arriving train. The model also will evaluate the number and

severity of the casualties and the impacts on the regional health care system. Combining the two models will yield estimates of deaths, injuries, service disruptions, physical damage to assets, and environmental effects concentrated on the rail system.

The third model, also supported by DOD, will estimate economic impacts from a failure of the transportation system to deliver people and products to their destinations; the estimates will include the monetary costs of deaths, injuries, and ecological impacts. The computable general equilibrium model will be able to simulate the impact on the New Jersey economy and will test options to reduce the impacts.

Cascading effects are likely to involve bottlenecks and congestion in local, regional, and national transportation and supply chains. For example, the economy eventually would adjust to the long disruption of a major rail station—people would try alternative paths of mass transit. But the mass transit system may lack the capacity, leaving many to opt for personal vehicles or to carpool, to change working hours, or to work from home.

The economic model also will estimate the economic impacts of investing in monitoring and surveillance, barriers, and other resilience measures, such as alternative ways of moving people and goods. Although diverting traffic to underutilized assets may take time, the effort could mitigate a long-run economic slide. The economic model will yield valuable insights for decision makers.



Screenshot from the industrial simulation model: corridor system map.

Spreading the Benefits

The direct beneficiaries of the models are NJ Transit, Amtrak, and freight rail operators in Northern New Jersey. The tools can help staff understand the vulnerabilities of the systems and the impacts of system disruption. In addition, rail system owners and operators outside the region will benefit by scaling the simulation models to their systems and regions.

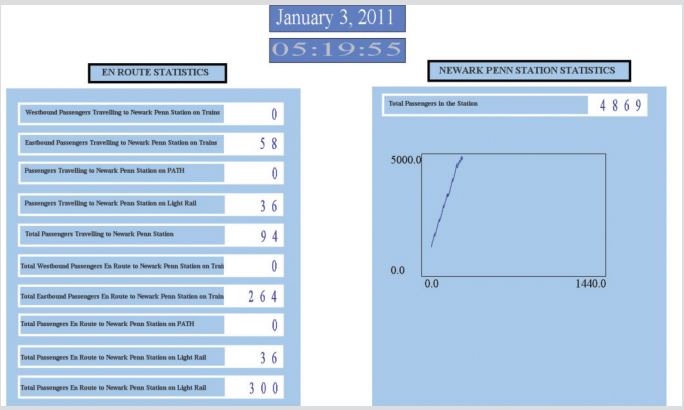
Other beneficiaries include the local, regional, and state departments that respond to all-hazards events: homeland security, law and public safety, health, and environmental protection. The models could be used, for example, in statewide strategic planning exercises focusing on response to rail-centered mass transit disasters.

Critical beneficiaries are the businesses and people dependent on a functioning rail system for the continuity of their livelihoods and commercial operations. Finally, the products will benefit educational programs in transportation security. The models can serve as tools for examining terrorist or all-hazard event scenarios in educational and training courses for transportation security and contingency planning.

Resources

Greenberg, M. R., T. Altiok, N. Fefferman, P. Georgopoulos, C. Lacy, M. Lahr, P. Lioy, K. Lowrie, H. Mayer, B. Ozbas, and F. Roberts. A Set of Blended Risk-Based Decision Support Tools for Protecting Passenger Rail-Centered Transit Corridors Against Cascading Impacts of Terrorist Attacks. White Paper for Department of Homeland Security University Summit, April 20, 2011; publication pending in *Journal of Homeland Security*.

Greenberg, M. R., K. Lowrie, H. Mayer, and T. Altiok. Risk-Based Decision Support Tools: Protecting Rail-Centered Transit Corridors from Cascading Effects. *Risk Analysis*, 2011. 10.1111/j.1539-6924.2011.01627.x.



Screenshot from the industrial simulation model: statistics page.

Greenberg is Professor and Associate Dean; Lowrie is Associate Director, Center for Transportation Safety, Security, and Risk (CTSSR); Lahr is Research Associate Professor; and Mayer is Executive Director, CTSSR, Rutgers University, New Brunswick, New Jersey. Altiok is Professor of Industrial and Systems Engineering, Rutgers University, Piscataway, New Jersey. Lioy is Professor, Robert Wood Johnson Medical School, Piscataway.

This research was supported by the U.S. Department of Homeland Security (DHS), Science and Technology Directorate, University Programs. The views and conclusions are those of the authors and do not necessarily represent the official policies of DHS.

SECURITY & CRITICAL INFRASTRUCTURE PROTECTION

Airport Security

Which Poses the Greater Threat—Passengers or Air Cargo?

RICHARD W. BLOOM

Photo: Werner Hennies, Munich Airport

The author is Associate Vice President, Academics, Embry-Riddle Aeronautical University, Prescott, Arizona, and chair of the TRB Aviation Security and Emergency Management Committee.

Which poses the greater threat to airport security—passengers or air cargo? This trick question assumes, first, an understanding of what security is; second, that airport security is a greater cause of concern than other kinds of security; and third, that the threat issuing from passengers and air cargo is stable. The question implicitly assumes that other entities are not a threat or not as threatening as passengers and air cargo, and that the threat must and should be avoided or minimized.

Examining these assumptions can clarify thinking about airport security from the perspectives of security professionals, security consumers, and purchasers or endorsers of security for the various modes of transportation. Although other security issues will be raised, terrorism is the focus.

Follow the Meanings

Sometimes airport security refers to a state of mind, a subjective state—that someone feels safe from intentional harm.[1] The actual situation at an airport—for example, the numbers of terrorist passengers, the types of bomb-laden cargo, the accuracy rates of the explosive detection systems, the type and duration of the training received by the behavioral detection personnel, and the functionality of a motion detector supporting perimeter security—may elicit different degrees of feeling safe from intentional harm at different times. The degree of feeling safe may have less to do with the actual situation at an airport than with personal, social, and professional aspects of one's life.

Airport security also may refer to an objective consequence—that someone is safe from intentional harm. Yet airport security personnel may not know this for certain, nor will terrorists or other criminals know how unsafe the airport is. As a result, deciding how much money to appropriate and allocate for airport security is difficult. Terrorists share a related problem: how much money and what expenditures will yield the greatest effect—for example, an attack via passengers, air cargo, both, or some other means?

A third meaning of airport security encompasses what is done to achieve the first two meanings—feelings of security and objective security. This includes measures such as behavioral detection,

[1] See Bloom, R. W. Fear of Flying: Globalization, Security, and Terrorism. *TR News*, July–August 2010, pp. 21–27.

PHOTO: DENVER INTERNATIONAL AIRPORT

A FedEx jet is loaded with cargo. Cargo security measures include explosives detection systems, known-shipper programs, and canine inspection.

The psychological effects of acts of terrorism—along with the more outwardly visible physical impacts—factor into any discussion of air security.

recognition, interviews, and interrogation; explosives detection systems; biometrics; profiling and data mining algorithms; known-shipper programs; and the older standbys of fences, locks, identifications, canine sniffers, package inspection, and cops walking the beat.

These three meanings of airport security provoke arguments and dysfunctional crosstalk among security experts confronted with operational challenges, policy issues, and budget recommendations. Answering the question of whether an airport has adequate security—and whether passengers or air cargo pose a greater threat—depends on security experts', terrorists', and the traveling public's perceptions of the three kinds of security and their vulnerabilities, their own perceptions, and their perceptions of the perceptions of the others. Ultimately, the question is which vulnerabilities, if successfully exploited, could achieve terrorist goals.

PHOTO: JACINTA QUESADA, FEMA

Security Worries

Worrying about airport security is helpful if the result is useful knowledge and action. But how much of airport security should be worried about? Some approaches to fix airport security could spend the entire U.S. federal budget but not reach perfection. Even if airport security were fixed, terrorists and other security violators could exploit a theoretically infinite number of other possible locations and situations that have vulnerabilities.

Examining the threats from passengers and air cargo and making recommendations to minimize the threats reveal the constraints of economic prudence and operational prudence. Terrorists who have adequate capabilities for intelligence, surveillance, and reconnaissance are aware of these constraints. The threat from passengers and air cargo will vary accordingly.

The Nature of Threat

Threat also may be defined as what may go wrong from passengers and air cargo, what will go wrong, and what is planned to go wrong through the means of passengers and air cargo—that is, an intentional threat from terrorists. Adding to the complexity is that a terrorist threat is both physical and psychological.

The psychological aspect involves the way that people cognitively, emotionally, motivationally, and behaviorally react to the physical, especially people whose reactions directly or indirectly may help achieve the political, religious, social, cultural, or other goals of terrorist planners and perpetrators. The meanings of a threat change according to the vulnerabilities of what is being attacked, as well as the probability and impact of a successful attack.

The comparison of threats from passengers versus air cargo, therefore, cannot yield a generic answer. Instead, the answer varies with interacting changes, including those in layers of security known and unknown to terrorists; social, cultural, economic, political, and environmental trends affecting terrorists and the world; and terrorist means, support, and motivations.

Comparing Sources of Threat

Even if accurate quantitative and qualitative analyses of the comparative threat from passengers and air cargo were possible, drawing a dichotomy between the two may itself pose a threat. Besides passengers,

human threats to airport security may come from airport workers, airline personnel, and the general public—including terrorists, terrorist supporters, and those who unknowingly become objects in terrorist plans and attacks—all with access to minimally screened areas and areas adjacent or proximal to the airport. Besides air cargo, inanimate threats to airport security may include commercial merchandise for sale, carry-on and checked baggage, weapons in minimally screened areas and areas adjacent or proximal to the airport, and exploitable natural disasters.

More appropriate and comprehensive, therefore, would be a comparative analysis of threat from people versus things—including terrorists and other criminal insiders, parking lot bombs, nonpassenger shooters in or adjacent to the terminal, portable air-defense systems proximal to the airport, and the biomedical threat from various populations. Again, terrorists' perceptions of security layers, larger trends, means, support, and motivations will affect the degree of threat—and this will change with time.

The main issues in identifying objective and intentional threat from passengers and air cargo in the context of terrorism involve the vulnerabilities that can be exploited by terrorists and that contribute to their choice of passengers and air cargo in attacks. Vulnerabilities known by terrorists in threat identification affect threat from passengers, air cargo, and any other means. Vulnerabilities in threat identification overlap with and contribute to basic target vulnerabilities—that is, what can go wrong, the probability that it will go wrong, and the impact on achieving terrorist goals.

Identifying Threat from Passengers

Identifying threat from passengers involves collecting and analyzing biological, psychological, and social information and developing a valid link to the probability of direct or indirect engagement in—or support of—terrorism. This applies to techniques such as data mining to collect and analyze travel history; biometrics, including facial recognition; human- and technology-mediated surveillance of mobility and location within the airport; behavioral detection and interviewing; or remote sensing of physiological activity. These techniques use the past and the present in an attempt to predict the future.

Predictions of human behavior, especially socially meaningful behavior, however, often are found wanting. More than 130 years of scientific psychological research suggest that the prediction of human social behavior is unknowable, even when the best practices of inferential statistical theories and the putative capabilities of human intuition, insight, and intelligence are applied.

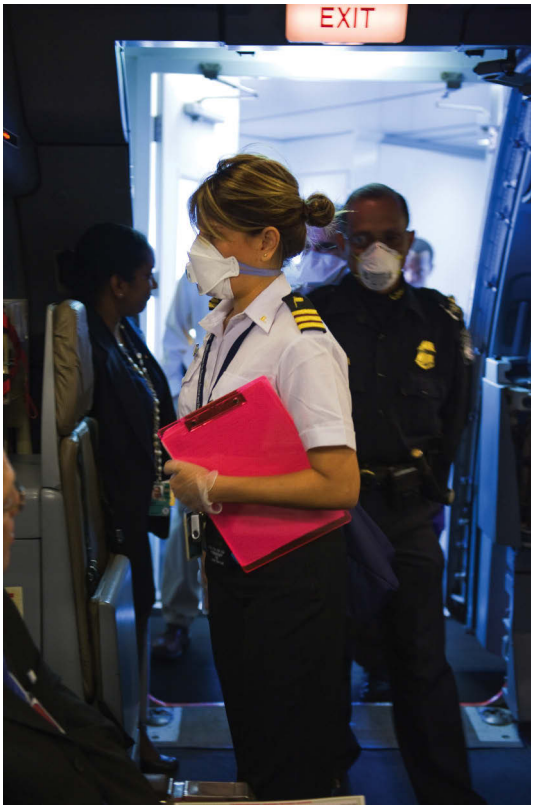


Photo: Christine Pearson, CDC

At an October 2008 preparedness exercise for various federal agencies, Centers for Disease Control and Prevention quarantine officer Danitza Tomianovic assesses the status of an ill traveler at the Miami International Airport. Threats from air passengers include the spread of disease.

Mass passenger screening poses 12 main difficulties:

1. The same data—the so-called signs, stigma, or indicators—may have different meanings at different times, in different situations, even with the same passenger, let alone different passengers.
2. The motivations of passengers may vary significantly within small temporal interludes, as may the links between motivations and specific behaviors.
3. How well can other people be known, if they themselves have less than complete conscious access to all motivations, which may vary?
4. Sophisticated passengers who intend terrorism will choose not to look like terrorists as described in watch lists and profiles, but like passengers who do not intend terrorist acts.
5. Most passengers are extremely unlikely to engage in terrorism; therefore a system to find terrorists must have extremely high sensitivity rates to identify terrorists, as well as extremely high specificity rates to avoid misidentifying nonterrorists as terrorists. Without high rates in sensitivity and specificity, operational chaos and a potential shutdown of commercial aviation would be likely.
6. Screening systems without high specificity rates may lead certain nonterrorist passengers to become terrorists because of perceived mistreatment.
7. Some terrorist passengers inevitably will be

PHOTO: GERALD NINO, CBP

A member of the U.S. Customs and Border Protection Beagle Brigade investigates a passenger's luggage for prohibited agricultural products. Dogs often are used as part of airports' security screening measures.

treated as nonterrorists—if the screening system lacks sufficiently high sensitivity—with successful terrorism as the result. Because of Points 4 through 7, random or modified random screening of passengers may be optimal, even including the proverbial 4-year-old child and the 90-year-old grandmother.

8. A common terrorist indicator, stress, is problematic. Passengers may be stressed for many nonterrorist reasons, such as trying to catch a flight, but may be calm about intentions to engage in terrorism in the service of God or to become a star through global news headlines.

9. The typical explanations for passenger terrorism, such as grievances and ideology, may only be the tip of the psychological iceberg. Security experts may be looking at what makes terrorist sense to the security expert, not to the terrorist.

10. All commonly accepted approaches to the prediction of terrorism have serious epistemological problems. Knowledge and logic both are affected by emotion and the unconscious, for good and for bad.

11. Research in psychology and philosophy suggests that the quest for valid mass screening of passenger terrorists based on appropriate mathematical procedures and linguistic concepts may be a waste of resources.

12. The sparse data available suggest that standoff crowd observations at best have minimal effect without time- and labor-intensive techniques including actual discourse between security personnel and each passenger identified for additional attention.

Vulnerabilities in Baggage Screening

In identifying the threat from passengers, the screening of carry-on and checked baggage, as well as clothing, possessions, and bodies, employs techniques that also are useful in screening air cargo. Although human security specialists may screen all of the above, as appropriate, with their eyes and hands, and dogs may screen with their sense of smell, more attention has centered on screening via technologies. This focus stems from the presumption that humans and dogs may take too long, may cost too much, may be disruptive to airport and aviation operations, and may be less accurate. These presumptions, however, are not always correct.

Technology-mediated screening is geared to identify physical characteristics of explosives, weaponry, and weapon components intended for terrorism. Bulk forms and trace amounts of proscribed materiel can be identified, with the immediate ascription of terrorist intent to the individual accountable. Technology-mediated screening usually analyzes an object's physical properties based on computerized algorithms. Differential densities of an object interacting with radiation, and explosives- and weapons-related particles interacting with chemical sensors, are the most common phenomena supporting detection.

Technology Problems

All technologies have problems, however. First, they are not 100 percent accurate in sensitivity and specificity and become less accurate in progressing from the experimental laboratory through field tests to operational deployment. Accuracy decreases further with human performance factors such as low motivation, fatigue, distractions, information anomalies, and dysfunctional heuristics.

Second, terrorist passengers supported by intelligence, reconnaissance, and surveillance capabilities may beat the system, work around it, or target another aspect of the airport or aviation, another transportation modality, or another venue. To counter this, security authorities may miscommunicate purposely about technologies or prepare altered technologies to fall into the hands of terrorists.

A third problem is that the costs are prohibitive. To field technologies at all airports and then to add the costs of installation, operations and maintenance, training, and the possibility of necessary structural and operational modifications to the airport can break a budget without preventing airport terrorism.

Opportunity cost also is involved, because the threat of passenger terrorism can weaken targets economically with few, if any, successful attacks. The increased security expenditure and overhead reinforces the perceived threat of attack and itself constitutes an attack.

Another cost involves the collateral economic damage of less efficient and enjoyable air travel for

recreation and business. The online and virtual worlds compete with aviation for revenue, often at lower cost, for entertainment and for work.

In addition, some technologies offend cultural sensibilities—for example, the wanding of a body or the opening of a coffin in transit. Cultural offense can increase motivations for terrorism in some passengers and can decrease the optimal performance of security personnel.

Some technologies also may pose health issues if the cumulative effects of screenings or possibly malfunctioning equipment generate higher exposure to radiation or chemicals—although the data to support these effects are not sufficient. These phenomena may present a significant threat, however, to the integrity of the contents of air cargo, along with associated damage to economic viability and trade.

The physics and chemistry of security technology may be poorly understood by security personnel, leading to misuse. A widespread belief in the magic of the technology supporting detection systems has hindered some security efforts. Terrorists intent on using passengers and air cargo in an attack can exploit the tensions between protecting proprietary information, the need for comprehensive vetting of a security process, and advocacy for relatively transparent methods in a representative democracy.

Air Cargo Threat

Passengers can be directly queried and physically appraised, but for air cargo only the people involved in the various processes from the creation of cargo through the many phases in the chain of custody can be queried. Much less attention and fewer resources have been addressed to the threat of air cargo than to the passenger threat. Many citizens and legal authorities seem to have less concern about aircraft carrying only cargo and a crew than about commercial passenger flights with cargo.

That air cargo containing explosive materiel or other noxious agents, whether on commercial passenger aircraft or on flights without commercial passengers, can endanger large numbers of people seems to be ignored, discounted, or repressed. Depending on the type of attack, the consequences could include large numbers of human casualties; a small number of casualties with high symbolic value; and symbolic, significant, and even catastrophic damage and destruction to communications, energy, and other infrastructure of national and international significance.

Identifying the objective and intentional threat from air cargo has vulnerabilities. The threat stems from the intentions of the planners of an attack, their perception of the vulnerabilities, and vulnerabilities of the target.

Cargo Screening Vulnerabilities

Air cargo varies in content, how the content is packaged and situated, and the configuration and other characteristics of the aircraft.

Content may be categorized by density, weight, size, economic value, and signatures of explosives, weapons, and weapons components. The associated screening challenges include (*a*) possible electrostatic discharge; (*b*) physical damage related to the method of screening; (*c*) levels of specificity and sensitivity related to the cargo content; and (*d*) terrorist knowledge of screening methods, which can lead to the development of countermeasures or to other means of exploitation.

Packaging is categorized by density, weight, size, and whether it is infiltrated with explosives or weapons materiel. Additional categories in the context of security include break bulk—individually loaded and unloaded items; palletized—items organized together on flat racks with netting, tensioned straps, and semistructural covers; and containerized—sealed receptacles categorized by height, width, depth, base, and maximum load. Packaging also is associated with combinations of tapes, locks, seals, tracking technologies, and sequenced methods for opening and closing, which pose strengths as well as vulnerabilities.

Important characteristics of aircraft configuration include the size, placement, thickness, and density of doors; the placement and dimensions of decks; the

PHOTO: WIKIMEDIA COMMONS

Fewer resources have been devoted to the issue of air cargo security. Cargo containing explosives or other harmful materials can endanger many people.

placement, dimensions, and number of holding compartments; and positions and procedures for situating cargo. Also of note are operating conditions; performance characteristics; structural and dynamic features; taxi, takeoff, and landing weights; fuel tanks; and engine, wheelbase, and fuselage characteristics. Any of these could be exploited as part of a terrorist attack.

Each of the main security approaches offers vulnerabilities—trace explosive detection; bulk explosive detection; canine explosive detection; detection devices for weapons and weapons components; education, training, and assessment for human operators of technology and for eye- and hand-mediated searches; and hardening of the packaging to mitigate an explosive threat from the contents.

Supply Chain Vulnerabilities

Many entities are involved in the air cargo supply chain, creating a significant vulnerability. A generic list of supply chain entities resembles the complexity of the final stanza of "The Twelve Days of Christmas": manufacturers, manufacturing facilities, freight forwarding facilities, shipping facilities, third-party logistics providers, warehouses, other distribution centers, independent cargo screening facilities, and more—the average number of entities handling a shipping container worldwide is 18, according to some experts.

The so-called known-shipper programs do not address the security of all involved in a shipment, and certified cargo prescreening programs do not address the security of the items shipped. The various screening methods chosen by government and business have significant error rates. Both the known-shipper and certified cargo prescreening programs incorporate vulnerability in the chain of custody, and both are exploitable by terrorists and other criminals, even with government-mandated inspections.

Security Conundrum

The physical and supply chain issues together create a conundrum. On one hand, implementing total and intrusive screening—which has dubious validity—could lead to significant cost in global economic viability, regardless of a successful terrorist attack; some opine that this economic damage constitutes the terrorist attack. On the other hand, partial and less comprehensive screening—also of dubious validity—could be more open to the economic catastrophe of a successful terrorist attack, but less open to global economic damage.

Of course, any correctly chosen and successfully implemented terrorist attack will cause global economic damage. These conclusions are not intended to damn security personnel and decision makers, but to underline the challenges they face.

Changing with Changes

The security threat from passengers or air cargo changes from moment to moment, depending on risk—the continuous coupling of threat with vulnerability, qualified by the impact and probability of a successful terrorist attack. The comparative analysis of the threat from passengers and air cargo raises five issues:

1. How effective are basic military, paramilitary, law enforcement, and intelligence operations to neutralize an attack before terrorists get anywhere near an airport? Information and intelligence need to be continuously and securely transmitted to aviation-related authorities to modify policies, plans, programs, and layers of security, moment by moment. The result can change the threat from passengers and air cargo, but also the planning preferences of terrorists—and can raise other fears.

2. Organizational psychology and human resource management—which involve morale, work culture, education and training, and personalities—can affect vulnerabilities in identifying the threat from passengers and air cargo. Organizational cultures can shape the perceptions of threat: the feelings of threat, the associated objective threat, and indirectly, the intentional threat from terrorists.

3. Foreign policy tools—diplomatic, economic, social, cultural, and humanitarian—should be used to shape international perceptions of the United States so that fewer people wish to engage in or support terrorism.

4. Too many people in the United States expect total safety and security—an unreasonable mass psychology that has not been addressed adequately by political and security leaders. Applying counterterrorism resources in ways that do not correspond to objective and intentional threat can render the United States an ever more lucrative terrorist target and can increase the probability of terrorist success—because objective success and objective failure both qualify as subjective success.

5. Terrorism ultimately is psychological. For example, public discourse and classified analysis of the comparative threat from passengers and air cargo are themselves part of the psychological battlefield, involving time, money, and attention working for and against terrorist goals.

In conclusion, the comparative threats from passengers and from air cargo will change as the world changes. As noted by many philosophers, we are of the world and in the world, part of the problem and part of the solution.

SECURITY & CRITICAL INFRASTRUCTURE PROTECTION

North American Perimeter Security

How Best to Keep Trade Moving?

MARY R. BROOKS

Official White House Photo by Pete Souza

Brooks is William A. Black Chair of Commerce, Dalhousie University, Halifax, Nova Scotia, Canada, and author of North American Freight Transportation: The Road to Security and Prosperity, *published by Edward Elgar.*

On February 4, 2011, U.S. President Barack Obama and Canadian Prime Minister Stephen Harper released the Beyond the Border vision of Canada–U.S. perimeter security. The vision renewed interest in refining and retuning the Canada–U.S. relationship in security, trade, and transportation:

> [W]e intend to pursue a perimeter approach to security, working together within, at, and away from the borders of our two countries to enhance our security and accelerate the legitimate flow of people, goods, and services between our two countries. We intend to do so in partnership, and in ways that support economic competitiveness, job creation, and prosperity.

History of Perimeter Security

Cooperation has been critical in the political relationship between Canada and the United States, from joint defense through NORAD to the Automotive Products Agreement, or auto pact, and the joint management of the St. Lawrence Seaway system. The long history of cooperation includes economic integration and management of joint assets and border infrastructure investment, as well as military cooperation and intelligence activities (*1*, Ch. 6).

(*Above:*) President Barack Obama confers with Canadian Prime Minister Stephen Harper at the G8 Summit in Muskoka, Canada, in June 2010. In February 2011, the two leaders released a declaration for a shared vision of Canada–U.S. perimeter security. (*Below:*) A U.S. Customs and Border Protection officer checks documents at the point of entry in Sweetgrass, Montana. Canada and the United States have a longtime cooperative relationship on border security.

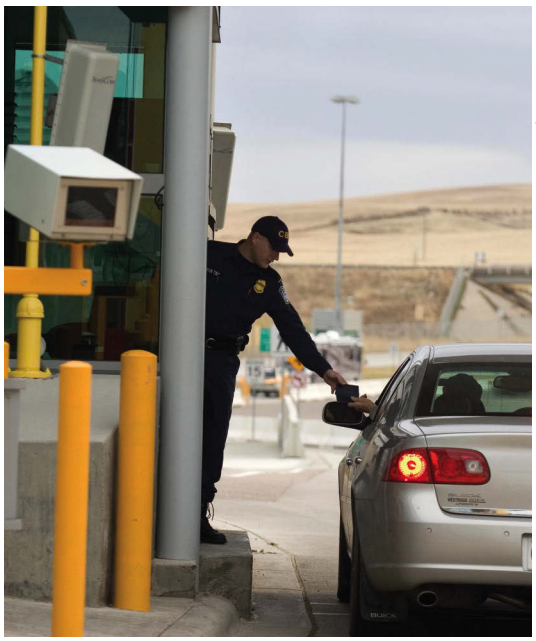


Photo: Gerald Nino, CBP

PHOTO: HSIA

Halifax Stanfield International Airport on September 11, 2001. Aircraft are parked on the second runway as gates are full.

The Fortress North America concept emerged during World War II when the two governments contemplated the unthinkable—that the rest of the world might fall to the Axis powers, and the United States and Canada would need to defend the continent. The resulting Permanent Joint Board of Defense and military cooperation continue today. Other milestones include the formation of NATO and the economic prosperity following the auto pact of 1965 and the Canada–U.S. Trade Agreement of 1987.

The United States and Canada have a common view for the defense of the continent. On September 11, 2001 (9/11), a Canadian was at the helm when military jets were scrambled in response to the World Trade Center attacks, and Canadian airports accepted diverted flights already en route to the United States.

The 1995 Canada–United States of America Accord on Our Shared Border was signed to promote trade, streamline procedures, and address smuggling and illegal entry. In 1999, the U.S. Customs Service launched the Canada–U.S. Partnership Forum to identify emerging border issues and promote dialogue to improve trade flows. The Canada–U.S. Transborder Working Group, established in October 2000 and jointly managed by Transport Canada and the Federal Highway Administration, focuses on border transportation management.

After the tragic events of 9/11, the two countries signed a long list of agreements affecting the northern border, with each agreement taking the commitments further and generating greater clarity on the extent of cooperation. The complexities of the challenges became more apparent, however, and many of the initiatives suffered from incomplete execution.

The tripartite 2005 Security and Prosperity Partnership (SPP) identified a myriad of activities, regulations, and agreements to address after the hardening of the northern and southern borders within the North American Free Trade Agreement (NAFTA) region. The process made clear that the same solutions would not necessarily work on both borders.

Although cooperation has not reached the same degree as among the European nations, with mutual recognition of practices and policies and the imposition of supranational regulations, progress on border issues between the United States and Canada has been steady, if not always effective. Both nations recognize that further improvements are needed if recovery from the global economic crisis is to favor the continent.

TABLE 1 Canada and U.S. Documentary Requirements for Freight

Import	Export
Bill of lading	Bill of lading
Certificate of origin	Commercial invoice
Commercial invoice	Customs export declaration form
Customs import declaration form	

SOURCE: *Trading Across Borders*, The World Bank, www.doingbusiness.org.

Integrating Economies

The global economic crisis has fostered a reexamination of sourcing strategies and supply chains, as each of the NAFTA countries also focuses on internal economic issues. The demise of the SPP in August 2009 made clear that traders no longer were confident that the partnership was effective as a forum to address trade flows and keep the NAFTA countries internationally competitive.

Trade data show that Canada's share of U.S. trade was 22 percent in 1993, 24 percent in 2004, and fell to 16 percent by 2010. The U.S. share of Canadian trade rose from 80 percent in 1993 to 84 percent in 2004 and fell to 70 per cent in 2010.

The integration of the two economies has been demonstrated; in many industries, products are made jointly—such as automobiles—but in others the integration only becomes obvious when a power failure occurs, as in August 2003, or a shortage arises, as of beef stock during the mad cow scare the same year. Yet the largest traders on the North American continent have not reaped the trade and transportation benefits that have accrued within the European customs union. The hardening of the border for security has affected trade.

The documentary processes for trade have undergone recent improvements. In 2009 the United States dropped the requirement for a packing slip for imports but added a certificate of origin. Canadian and American documentary requirements for trade are now harmonized (Table 1, left).

Nonetheless, security concerns incur significant transaction costs for trade and affect economic well-being. When Canadian and U.S. logistics performance indicators are benchmarked against those of top-ranked Germany, some of the gaps are wide (Table 2, next page). Both countries need to reduce the gap with Germany in performance benchmarks; one way would be to address the transaction costs at the border. In addition, delay along the northern border is a key cost of doing business for both countries.

TABLE 2 Logistics Performance Indicators: Germany, Canada, and the United States

Rank	Country	LPI	Customs	Infrastructure	International Shipments	Logistics Competence	Tracking & Tracing	Timeliness
1	Germany	4.11	4	4.34	3.66	4.14	4.18	4.48
14	Canada	3.87	3.71	4.03	3.24	3.99	4.01	4.41
15	U.S.	3.86	3.68	4.15	3.21	3.92	4.17	4.19

NOTES: LPI = composite logistics performance indicator; customs = efficiency of customs clearance; infrastructure = quality of trade and transport infrastructure; international shipments = ease of arranging competitively priced shipments; logistics competence = competence and quality of service provided; tracking = ability to track and trace shipments; timeliness = reaching destination within scheduled or expected delivery time.

SOURCE: Logistics Performance Indicator, The World Bank, 2011, http://go.worldbank.org/88X6PU5GV0.

The Cost of Delay

Many studies in the past 10 years have attempted to quantify the costs of delay at the Canada–U.S. border. Several have demonstrated that the border has a serious cost to both trade and transportation (*2–4*). Yet delay at some crossings was problematic before 9/11 security concerns. In 2000, the cost of delay at the Ambassador Bridge connecting Detroit, Michigan, and Windsor, Ontario, was estimated at US$135.6 million to US$180.6 million for truck trips from Canada to the United States (*4*). In 2001, before the terrorist attacks, crossing the Canada–U.S. border increased the cost of Canadian manufactured goods by an average of 6 percent, when no tariffs were being collected (*5*).

A 2003 study estimated the cost of crossing the border at US$382.0 billion, or 2.7 percent of total 2001 U.S.–Canada trade in goods (*3*). A 2004 follow-up demonstrated that greater uncertainty was leading buyers to reconsider sourcing decisions, although the crossing times were not dramatically different (*6*). The study found, however, that transborder trucking freight rates were 10 to 35 percent higher.

A 2005 report concluded that truck delay was the biggest component of the costs of compliance with security programs (*2*). The report noted that the cost was mitigated by industry's ability to impose offsetting surcharges, usually passed on to the consumer, making the product less price-competitive.

With the tighter management of global supply chains in the past decade, uncertainty in border crossing times has taken a toll on the competitiveness of those who depend on the transborder movement of goods. Recent studies on the Pacific Highway (*7, 8*) and on the southern Ontario access

PHOTO: MIKE RUSSELL

Delays at the border can become expensive—research indicates that in 2000, the cost of delays at the Ambassador Bridge between Michigan and Ontario was estimated from US$136 million to US$181 million for truck trips into the United States.

points (*9*) have explored the challenges of continued delays and the causes of variability in the delays, but without providing solutions for reducing the cost beyond programs like the Free and Secure Trade, or FAST, program.

The addition of fees and inspections, along with increases in security regulations and processes, has added to the administrative and financial burdens for all who trade with and transport goods to and from the United States. Although enhanced security is necessary to respond to terrorism and organized crime, the availability of technologies such as global positioning systems and radio frequency identification tags, along with computer-enhanced documentation, should offset these burdens.

Border delay continues to be a key issue in the latest discussions about perimeter security. Although the new Beyond the Border Working Group will enable security officials to address issues of crime, migration, and health, the coverage needs to extend to trade flow improvements to achieve perimeter security.

Perspectives on Perimeter Security

The interpretation of perimeter security varies with perspective. The perspectives of an importer and of consumers or citizens illustrate this.

Importer's Perspective

A Toronto importer has many transportation and routing options to acquire goods. For example, the cargo may come from China directly to Canada via the Port of Vancouver, or it may come via the Port of Long Beach, California, and cross a second border to enter Canada. With seamless perimeter security, the Toronto importer would expect that the Chinese-manufactured goods arriving via Long Beach could clear customs once and not be delayed at the Canada–U.S. border.

The second border clearance, however, may not be seamless, because regulatory burdens and a lack of harmonized standards within North America work against a two-border routing. If the second clearance is seamless and not held up by the regulatory and jurisdictional differences, then the risk for the Toronto importer in choosing a Long Beach routing is reduced, if not completely mitigated.

By extension, a seamless border arrangement broadens the reach of California companies by opening the Canadian market as if shipping to Chicago. A Chicago importer buying goods in Ontario, or in China or India via Vancouver, faces a similar situation. The reduction in transaction costs improves the competitiveness and market reach of North American suppliers.

Consumer's Perspective

The Canadian citizen may view the perimeter security agreement as Americans denting Canadian constitutional rights on immigration and gaining access to private data. For this reason, the Industry Canada website notes that privacy rights will be respected in Beyond the Border commitments.

American concerns about who receives citizenship in Canada appear to be more important than concerns about economic prosperity. The lack of trust on security overshadows recognition of possible economic benefits.

At a Transportation Research Board 2011 Annual Meeting program session, North American Border Issues and Trends, immigration expert Deborah W. Meyers of the Department of Homeland Security noted that Canadians seem to hold Americans responsible for the northbound flood of cocaine, cash, and tobacco, while Americans see Canadians as the southbound source of cheap marijuana and ecstasy. This illegal activity is a shared problem that a coordinated approach to perimeter clearance could resolve.

The full implementation of trusted shipper programs, common technological standards, and other promises in the perimeter security announcement imply that fewer resources would be allocated to hardening the border and duplicating personnel, and more would address such shared challenges as halting the drug trade and enhancing trade flow through

Recent studies on the Pacific Highway border crossing from Washington, United States, to British Columbia, Canada, have probed causes and variability of border delays.

Photo: Sam Cazon

Photo Courtesy of the Port of Long Beach

A seamless border arrangement between the United States and Canada would allow goods to be imported more efficiently from places like Asia.

infrastructure investments. Mutual recognition of standards and technology could be a powerful force but does not appear on the agenda of the Beyond the Border declaration.

Refocusing Resources

If the two countries share a commitment to make the border more fluid and reliable, agreeing on standards of technology and transportation, economic prosperity will increase as transaction costs are reduced. The U.S. Government Accountability Office Report 10-106 documents Department of Homeland Security challenges in scanning containers, administering the Transport Workers Identity Credential, and enforcing cybersecurity. Full-fledged adoption of mutual recognition within a secure perimeter would help the United States find the resources to focus on security challenges outside the perimeter. Without a commitment to perimeter thinking, tinkering with security will take much longer to reach the goal of a more secure region.

Trade and transportation issues are being held up by those who do not understand the supply chain and fear the worst of their neighbors. Although mobility across the border has been a core tenet of U.S.–Canada cooperation since the 1930s (*10*), mobility has not necessarily bred familiarity or the understanding necessary for a common perimeter to work.

Shared Vision Framework

The 2011 declaration, A Shared Vision for Perimeter Security and Economic Competitiveness, implies that negotiations between the two countries will provide a framework for joint threat assessment, intelligence gathering, and information sharing, as well as a commitment to cross-border law enforcement targeting transnational crime. A four-pronged approach is planned:

- Address early threats;
- Facilitate trade, economic growth, and job creation;
- Integrate cross-border law enforcement; and
- Enhance critical infrastructure protection and cybersecurity.

Each initiative has the potential to improve the trade and transportation relationship.

Canada–U.S. agreements will be updated to incorporate the initiatives. The Agreement Between the Government of Canada and the Government of the United States of America on Emergency Management Cooperation, updated in 2008, and the Canada–U.S. Framework for the Movement of Goods and People Across the Border During and Following an Emergency, signed in 2009, will play key roles in a risk management approach that envi-

Photo: Brandon Blackwell, U.S. Coast Guard

Royal Canadian Mounted Police and U.S. Coast Guard officers conduct Shiprider law enforcement operations along the Niagara River during the G20 Summit in June 2010.

sions cooperation between agencies and agreement on intelligence gathering and information sharing.

Border Risk Assessment

The March 2011 release of the Joint Border Threat and Risk Assessment already has supplemented the declaration. Part of a shared vision for border security, the assessment provides U.S. and Canadian policy makers, resource planners, and law enforcement officials with a strategic overview of the threats along the 5,525-mile (8,891-kilometer) international boundary between the United States and Canada, and reflects a commitment to work together to "safeguard both nations' vital assets, networks, infrastructure, and citizens."

The threat assessment specifies categories of risks: national security, criminal enterprises, migration, agriculture, and health. On the table are joint activities that go beyond the physical movement of goods and people: cybersecurity, health security, critical infrastructure protection, common standards on biometrics, and common procedures for customs processing and regulatory compliance, as practicable. The plan is to address transnational crime, including smuggling, organized crime, and mass marketing fraud.

A key feature is the establishment of Integrated Border Enforcement Teams (IBETs) of Canadians and Americans to share information and resources across five core agencies. Although IBETs have been at work since 1996, the initiative reinforces activities such as the Customs and Border Protection teams in Canadian ports and the joint enforcement teams of the Shiprider program on the Great Lakes.

Infrastructure Investment

From a transportation perspective, the Beyond the Border vision assures a focus on "investment in modern infrastructure and technology at our busiest land ports of entry." The initiative promises "organizing binational port of entry committees to coordinate planning and funding, building, expanding, or modernizing shared border management facilities and border infrastructure where appropriate, and using information technology solutions."

The commitment to invest in infrastructure and technological solutions will smooth trade flows between the two countries. The border may be less hard but will be more secure through the extension of trusted traveler and supplier programs and through streamlined advance documentation. These are high goals for two countries with key differences in governance and jurisdiction for these activities.

Regulatory Cooperation

The land border commitments do not mean that the strategy is land based and inside the perimeter or that marine and air ports of entry into the secured perimeter of a Canada–U.S. region will lack coordinated effort. The declaration indicates the two countries will cooperate by developing

> an integrated cargo security strategy that ensures compatible screening methods for goods and cargo before they depart foreign ports bound for the United States or Canada, so that once they enter the territory of either we can, together, accelerate subsequent crossings at land ports of entry between our two countries.

Key to this vision is the creation of a United States–Canada Regulatory Cooperation Council (RCC), composed of senior regulatory, trade, and foreign affairs officials from both governments: "The RCC has a two-year mandate to work together to promote economic growth, job creation, and benefits to our consumers and businesses through increased regulatory transparency and coordination." Not addressed, however, is the long-standing lack of regulatory harmonization on such issues as vehicle size and weights, driver hours of service, or any of the other divergences of transportation regulations documented in *North American Freight Transportation* (*1*).

The government of Canada established a website for public comment from March 13 to April 21, 2011. A report summarizing the findings will be published later in the year. In the United States, the Department of Commerce gathered public comment via the *Federal Register* from March 3 through April 4.

Photo: Gerald Nino, CBP

The United States has a de facto two-border policy—tighter controls at the U.S.–Mexico border (pictured) and more open ones at the border with Canada.

Keeping Trade Moving

In 2003, Stephen Flynn proposed that the United States adopt a two-border policy: hardening the border with Mexico and opening the border with Canada, similar to the concept of perimeter security (*11*). The proposal supported effective targeting through anomaly detection and prescreening to identify low-risk players.

Flynn noted that a closed border is tantamount to a self-imposed embargo—a win for the terrorists, because the victim has implemented action against itself. A hardened border has other unintended consequences: the tighter controls and security provide criminals with incentives to make arrangements with, and to prey on, low-paid security staff. The failure to deliver trilateral border benefits has led to a de facto two-border policy.

References

1. Brooks, M. R. *North American Freight Transportation: The Road to Security and Prosperity.* Edward Elgar Publishing, 2008.
2. DAMF Consultants and L.-P. Tardif & Associates. *Final Report: The Cumulative Impact of U.S. Import Compliance Programs at the Canada–U.S. Land Border on the Canadian Trucking Industry*. Transport Canada, Ottawa, May 24, 2005.
3. Taylor, J. C., D. R. Robideaux, and G. C. Jackson. The U.S.–Canada Border: Costs Attributable to the Border and Trade Policy, and the Implications for an External Perimeter Strategy. *Canadian Transportation Research Forum Proceedings*, Vol. 1, pp. 228–242 (2003).
4. Belzer, M. H. *The Jobs Tunnel: The Economic Impact of Adequate Border-Crossing Infrastructure*. Sound Science, Ann Arbor, Mich., 2003.
5. Trickey, M. The Undefended Border: Economic Concerns Spur Campaign to Erase Line Between Us and the U.S. *Montreal Gazette*, Aug. 4, 2001, p. A12.
6. Taylor, J. C., D. R. Robideaux, and G. C. Jackson. Costs of the U.S.–Canada Border. In *North American Economic and Financial Integration* (*Research in Global Strategic Management*, Vol. 10), A. M. Rugman (ed.), Elsevier, Oxford, 2004, pp. 283–298.
7. Goodchild, A., L. Leung, and S. Albrecht. Free and Secure Trade Commercial Vehicle Crossing Times at the Pacific Highway Port of Entry. *Journal of Transportation Engineering*, Vol. 136, No. 10, pp. 932–935.
8. Kristjánsson, K. Á., M. Bomba, and A. V. Goodchild. Intra-Industry Trade Analysis of U.S. State–Canadian Province Pairs: Implications for the Cost of Border Delay. In *Transportation Research Record: Journal of the Transportation Research Board, No. 2162,* Transportation Research Board of the National Academies, Washington, D.C., 2010, pp. 73–80.
9. Anderson, W. P., and A. Coates. Delays and Uncertainty in Freight Movements at Canada–U.S. Border Crossings. *Canadian Transportation Research Forum Proceedings*, May 30–June 2, 2010, pp. 129–143.
10. Ginsburg, S. Securing Human Mobility at the U.S.–Canada Border, *National Strategy Forum Review*, Vol. 19, No.3 (2010). http://nationalstrategy.com/Portals/0/documents/Summer%202010%20NSFR/Susan%20Ginsburg-Summer%202010%20NSFR.pdf.
11. Flynn, S. The False Conundrum: Continental Integration Versus Homeland Security. In *The Rebordering of North America: Integration and Exclusion in a New Security Context*, P. Andreas and T. J. Biersteker (eds.), Routledge, New York and London, 2003, pp. 110–127.

Supporting Secure and Resilient Inland Waterways

HEATHER NACHTMANN

The more than 25,000 miles of the nation's inland waterways transport millions of tons of cargo every day. The U.S. Army Corps of Engineers (USACE) is responsible for nearly 12,000 miles of the most commercially important waterways—the Mississippi–Ohio River System, the Gulf Intracoastal Waterway, the Intracoastal Waterway along the Atlantic Coast, and the Columbia–Snake River System in the Pacific Northwest. According to USACE, the coal transported on the inland waterway system—approximately 20 percent of the nation's output—produces 10 percent of all electricity used in the United States annually. The waterways also transport more than 20 percent of U.S. petroleum and petroleum products and 60 percent of the nation's farm exports.

Photo: Patrick Moes, U.S. Army Corps of Engineers

Train depot flooded by the Mississippi River, Vicksburg, Mississippi, May 13, 2011.

Disruption to the inland waterway transportation system, therefore, can cause significant economic losses. According to CBS News, the chief executive officer of the Port of New Orleans estimated that closing the Mississippi River for one day would cause an economic loss of $300 million. Because much of the cargo shipped by barge consists of raw materials for other industries, disruptions in barge transportation affect production and cause economic losses throughout the country. Lynn Muench of the American Waterways Operators likened the river closures and restrictions during and after the May 2011 floods to the effect that "tearing down all the bridges across the Mississippi River [would have on] the trucking industry."

Photo: U.S. Army Corps of Engineers

Floodwaters from the Mississippi River flow through bays at the Morganza Spillway in Louisiana, May 14, 2011.

A typical tow comprises dozens of barges, each with a capacity of approximately 60 truckloads. Rerouting disrupted cargo without overwhelming an already congested highway system presents a challenge.

Research teams at the Mack-Blackwell Rural Transportation Center at the University of Arkansas and at the Center for Transportation Safety, Security, and Risk at Rutgers University are working to mitigate economic and societal losses by developing guidance on prioritizing disrupted cargo for moving off the rivers. The prototype decision support system integrates geographic information system technology and computer-based freight movement models to provide timely identification of cargoes that should be given priority for offloading during a response to an emergency, such as an attack or natural disaster on the inland waterway. The prototype system sets the priorities for offloading waterborne cargoes based on economic impacts and societal requirements and assigns the prioritized freight for transport via rail and truck based on available freight capacities.

Conducted through the U.S. Department of Homeland Security National Transportation Security Center of Excellence, the project seeks to develop a fundamental understanding of the interdependence of critical multimodal transportation infrastructure systems and their associated cargo and of the ability of land-based transportation systems to respond quickly to catastrophic events that may occur on the inland waterway system.

The resiliency of the inland waterway system is a function of its infrastructure, including locks and bridges; of its physical characteristics, such as channel widths and the merging and dividing of tributaries; and of the ready access to ports and land-based transportation systems with adequate capacity to receive and move offloaded materials and goods after a disruption on the waterway. The training and ability of managers and operators to shift to alternative paths also is important. The project is scheduled for completion in summer 2013.

The author is Director, Mack-Blackwell Rural Transportation Center, and Associate Professor of Industrial Engineering, University of Arkansas, Fayetteville.

This article describes work supported by a grant from the U.S. Department of Homeland Security.

POINT OF VIEW

Maritime Security, Piracy, and the Global Supply Chain

STEPHEN CARMEL

The author is Senior Vice President, Maersk Line, Limited, Norfolk, Virginia.

When someone says "maritime security," the general reaction is to think of pirates. Piracy has become almost synonymous with maritime security, displacing the previous threat to global shipping, the dirty bomb in a box.

Piracy has had limited—if any—impact on global supply chains and zero effect on supply chains critical to the United States. No one has articulated U.S. national interest beyond general stability in Africa and the U.S. role as global cop. An obsession with piracy, however, distracts attention from the myriad of other threats to world trade and maritime security. When one of those other events occurs, the term "black swan"—signifying something dramatically unexpected—inevitably appears in the analysis. Yet an assessment of the state of global affairs would find that a flock of black swans is on the way.

Security's Value

Maritime security—or any security—is pointless in and of itself. The value of maritime security is in what it is intended to protect. Trade and the goods and services that flow through the system are essential to the welfare of American society. If protecting the global supply chains somehow chokes them off, victory has been handed to those who intend harm. Perfect security comes at such a steep cost that achieving it will represent a win for the bad guys. Resiliency, the ability to recover quickly, denies bad guys what they are after while keeping the focus on what is being protected instead of on the mechanics of protection.

According to a popular saying, good guys need to be successful every time; bad guys only need to be successful once. Bad guys, however, only need to raise the worry that they might be successful, leveraging irra-

PHOTO: JASON R. ZALASKY, U.S. NAVY

A team from the amphibious dock landing ship USS *Ashland* inspects a skiff in the Gulf of Aden for suspected pirate activity. Piracy is just one threat among many to maritime security.

PHOTO: GERALD NINO, CBP

The U.S. Customs and Border Protection (CBP) New Mobile Sea Container System for screening cargo. This and other CBP container screening processes depend on a secure flow of information.

tional fear, which causes more damage than they could do on their own. A Booz Allen study is widely cited as determining that a 10-day shutdown of U.S. ports from a dirty bomb attack caused $58 billion in economic damage and required 90 days to clear the backlog (*1*). The attack failed, and the bad guys did zero damage directly—the damage was done by U.S. authorities reacting to the failed attempt.

No one wants to suffer at the hands of bad guys, but suffering because of bad policy also should be avoided. A European Commission study found that if 100 percent scanning were enforced, and the practice spread to global trading partners, the deadweight loss to the world economy would approximate €150 billion per year (*2*)—far more damage than pirates will ever do; moreover, 100 percent scanning ultimately would make global supply chains less secure, not more.

A Congressional Research Service (CRS) analysis noted that the economic effects of the terrorist attacks of September 11, 2001 (9/11), were transitory: "Notwithstanding their dire costs in human life, the direct effects of the attacks were too small and too geographically concentrated to make a significant dent in the nation's economic output" (*3*). According to the report, the economic consequences were the deleterious effects of enhanced security policy on the global economy, including a reduction in growth, as resources were channeled to security measures.

Bad guy attacks are a low-probability, high-consequence event, while bad policy is a medium-consequence, but high-probability, event; moreover, bad policy is easy to inflict and hard to remove once in place. Trust and public–private partnering are essential to achieve the delicate balance between the flow of commerce and good security policy.

POINT OF VIEW presents opinions of contributing authors on transportation issues. The views expressed are not necessarily those of TRB or TR News. *Readers are encouraged to comment in a letter to the editor on the issues and opinions presented.*

Network Dynamics

The marine transportation system (MTS) operates in accordance with well-defined network dynamics. The MTS itself is part of a larger system with a different set of network dynamics. Trade often consists more of component parts destined for another factory's assembly line than of finished goods ready for retail. The Japanese earthquake in March showed how quickly supply chains can be disrupted, as factories in the United States closed within a week of the earthquake because of a lack of components from Japan.

The MTS cannot be treated as a set of discrete parts; disaggregating components to analyze system behavior does not work. Yet this approach usually is applied to maritime security—for example, in deciding when, where, and how to fund port security programs. Propagated effects characterize these types of networks; where the attack happens and where the results are felt most severely are not always the same. In other words, not all parts of the system are equal,

and system effect, not ease of physical attack, should determine the allocation of resources.

A cyberattack on the computer systems that manage rail traffic can have as much impact on the flow of commerce through a port as a bomb on a pier. Links between nodes, modal interdependency, cascading failure, propagated effects, and network system dynamics are well understood in network theory and are applied to infrastructure resiliency studies, such as analyses of power grid vulnerability, but are absent from the MTS security discussion.

Vulnerability is not measured by the physical ease of attack, but by the systemic effect. The political process may pose hindrances in addressing vulnerability; for example, a politician from Florida may be unlikely to concede that Norfolk, Virginia, or Charleston, South Carolina, is more important from a system perspective than ports in Florida and therefore should receive more port security dollars; others may balk at using maritime security dollars to protect railroads. Adding to the problem is that no single federal agency is charged with understanding and protecting critical global supply chains as interconnected, interdependent systems.

Cybervulnerability

A byword in the security dialogue holds that 90 percent of international trade moves by water. The statement applies correctly to trade in physical stuff, excluding intra-European trade. In terms of value, however, 60 percent to 70 percent moves by water.

Approximately 20 percent of total trade is in services that largely move via fiberoptic cable (4). Cyberwarriors are protecting the smooth flow of trade as much as the U.S. Navy or Coast Guard are. Moreover, trade in physical stuff cannot occur without the smooth flow of information and a secure Internet. In linked systems displaying network dynamics, indirect attacks via propagated effects can be damaging, yet difficult to detect; the financial system, for example, is cyberdependent. Underestimating the vulnerability of the MTS system to cyberattack, such as information corruption, would be a mistake.

The U.S. Customs and Border Patrol (CBP) process for screening containers depends on the secure international flow of information. If CBP lost confidence in the information systems for the 10+2 cargo data program, for example, the inbound container screening process and the flow of goods through U.S. ports would be affected.

Another source of vulnerability is the Global Positioning System (GPS); the MTS depends on GPS not only for positional information but for the timing signal, used to control many industrial processes, including the electrical grid and financial systems. A disruption in the GPS could halt trade.

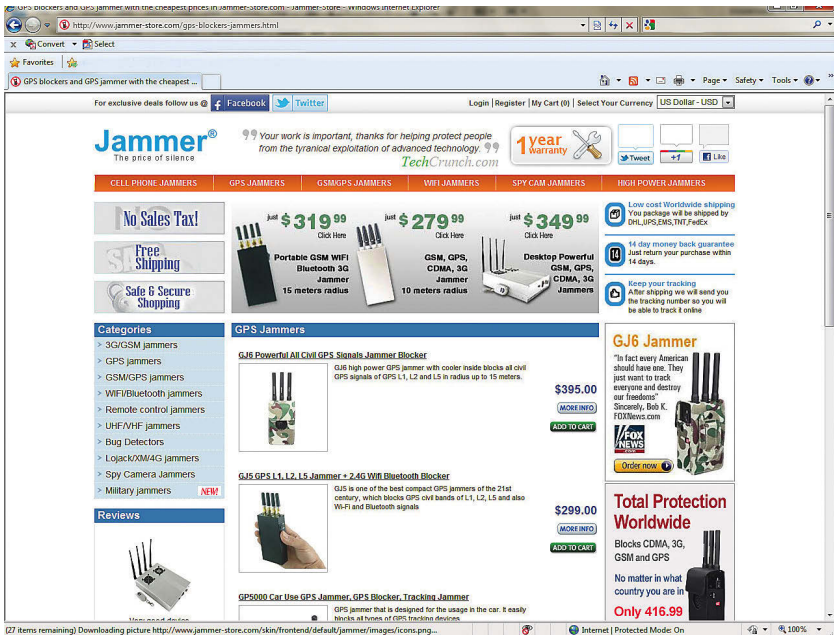
A report from the Royal Academy of Engineering in the United Kingdom notes that "the European Commission has estimated that…6 percent to 7 percent of gross domestic product in Western countries, that is to say €800 billion in the European Union, [depends] on satellite radio navigation" (5). In the United States, the Government Accountability Office (GAO) has criticized the U.S. Air Force program to maintain and modernize the GPS satellite constellation (6).

GPS jammers are available via the Internet; one advertisement notes that a $30 GPS jammer made in China can "ruin your day," creating a "moving cloud of chaos." Taking the continued availability and accuracy of the GPS for granted and failing to anticipate the potential impacts of a failure represents another black swan on the wing.

The potential for so-called supervisory control and data acquisition, or SCADA, attacks to cause direct physical damage to critical nodes or equipment in the MTS represents another significant threat. A Stuxnet type of attack on critical controls in the MTS is possible, and the potential for an attacker to tap into ship controls via the satellite communication system should not be ruled out. The Stuxnet worm demonstrated that physical proximity is not necessary to achieve physical damage.

Critical Materials

Much high-value material moves principally by air—a reminder of the intermodal nature of international supply chains. In the Japanese earthquake, many of



GPS jammers are readily available online, pointing to the vulnerability of a key technology for navigation, industry, and trade.

The guided-missile destroyer USS Bainbridge tows a lifeboat from the Maersk *Alabama* to an amphibious assault ship to be processed for evidence after the successful rescue of Richard Phillips, who was held by suspected Somali pirates for 5 days after a failed hijacking attempt off the Somali coast. Less than 2 percent of U.S. commerce is carried on U.S.-flag ships such as the *Alabama*.

the first supply chains to fail were those that used air as the principal mode of transport—these have the fastest cycle time and display effects faster than others. Another example is the catastrophic impact the Iceland volcano and the closure of European airspace had on farmers in Kenya. The United States imports a large amount of critical material by air, including electronics and pharmaceuticals; the aviation supply chain is complex and unforgiving.

The United States is the world's third largest oil producer, after Saudi Arabia and Russia, and has the world's largest reserves of total fossil fuels, more than twice that of Saudi Arabia (*7*). U.S. dependence on foreign suppliers of oil is more a matter of technology than resources.

Switching to nuclear energy will not end U.S. reliance on foreign suppliers of energy. According to data from the Energy Information Agency, the United States imports approximately 85 percent of the uranium used in commercial nuclear power plants; approximately 40 percent of these imports come from Russia (*8*). The United States is more dependent on foreign suppliers of uranium for nuclear power than on foreign suppliers of oil—imports meet approximately 50 percent of petroleum needs. Switching to nuclear energy, therefore, would not end a supply-chain vulnerability. Substituting a known vulnerability for unknown vulnerabilities with effects that cannot be mitigated would make the supply chain—and society—less secure.

The United States also imports other critical materials. For example, China is the world's sole supplier of processed rare earths, elements essential for permanent magnets and lightweight electric motors. Rare earths are needed in making cruise missiles, JDAMS or smart bombs, Sidewinder air-to-air missiles, the AN/SPY-1 naval radar system, and some targeting systems.

Legislative Threats

Another, but indirect, threat to maritime security is protectionist legislation to promote national security. Legislation that attempts to insulate the United States from the world will only provide a false sense of security, may provoke retaliatory measures from trade partners, and will raise the stress level in the trade system.

The U.S. economy remains the world's largest manufacturer, although a March 2011 IHS Global Insight report noted that China had taken a slight lead in manufacturing output (*9*). The report compared output based on nominal dollar value, which is influenced by the exchange rate. Measured in terms of the manufacturing value-added component of the gross domestic product, which is not influenced by exchange rates, the U.S. output roughly amounts to a 21 percent share of global manufacturing, with China second at 15 percent (*10*).

Although China is slightly ahead of the United States in terms of the nominal dollar value percentage of world manufacturing output—19.8 percent to 19.4 percent—China requires 100 million workers to produce an output roughly equivalent to what the United States produces with 11.5 million workers. The U.S. advantage in productivity—and standard of living—is astounding, ranking as the world's second most competitive economy, after Switzerland, and the world's third largest exporter, behind China and Germany. The United States, therefore, would suffer if trade wars got out of hand.

Globalization and disaggregated supply chains mean that U.S. manufacturers rely heavily on imported components to keep assembly lines and manufacturing plants open. A significant portion of imported container trade consists of component materials destined for further processing in U.S. factories; the "made in" label plate is becoming meaningless. Interruptions anywhere in the supply chain, in any mode, and for any reason—bad guys or bad policy—will lead rapidly to U.S. unemployment, social stress, and political backlash.

As noted, this was demonstrated on a small scale

Photo: Megan E. Sindelar, U.S. Marine Corps

in the aftermath of the Japan earthquake, when U.S. factories closed for lack of component parts made in Japan. The largest customer for containerized U.S. exports is China, at 2.3 million TEU (20-foot equivalent units) in 2009—roughly three times as much as the next largest customer, Japan. The largest U.S. container export customer outside of Asia is Belgium, the seventh largest destination, with approximately 250,000 TEU per year (*11*).

U.S. policy makers should recognize that the nation's top six customers are in Asia, where interconnected supply chains and manufacturing processes are deep and complex. Trade sanctions against one nation are trade sanctions against many. China is one of the biggest agricultural customers for the United States, tying Mexico for second behind Canada, as of February 2010. Maritime security is not only about making sure that what is needed arrives here, but that what the United States sells reaches its destination, which increasingly is China. Again, the biggest threat to that trade is bad policy.

Piracy's Threat

Piracy is an issue that merits attention, but the discussion has failed to examine the problem from a system perspective. The words of the CRS report on the 9/11 attacks apply to piracy: "The direct effects… [are] too small and too geographically concentrated to make a significant dent in the nation's economic output." Piracy is analyzed through the lens of specific events, but policy should focus on system-level effects. Two distinct aspects should be considered: the direct national interest of the United States and the interest of the global commons.

In a speech at George Washington University in April 2011, President Obama spoke about the Department of Defense budget: "We need to not only eliminate waste and improve efficiency and effectiveness, but conduct a fundamental review of America's missions, capabilities, and our role in a changing world." This approach is applicable to the issue of combating piracy—that is, the U.S. national interest should be the focus when contemplating where to expend scarce defense dollars.

The threat from piracy to U.S.-flag shipping is minimal—less than 2 percent of U.S. commerce is now carried on U.S.-flag ships (*12*). U.S.-flag shipping, such as the Maersk *Alabama*, mostly is engaged in carrying food aid or Department of Defense cargo—not in foreign commerce.

Comparisons with the Barbary pirates and Thomas Jefferson's response are invalid (*13*). At that time, the U.S.-flag merchant marine was the largest in the world and carried more than 90 percent of U.S. foreign commerce; Barbary piracy represented a threat to the young republic that demanded a robust response. Today the threat of Somali piracy to U.S. foreign commerce and economic well-being is nil.

Trade with Asia favors the U.S. West Coast, and U.S. commerce passing Somalia travels on ships too big and too fast to be vulnerable to piracy. Approximately 13 percent of U.S. oil imports flow from the Persian Gulf area, traveling around Africa instead of via the Suez Canal, not to avoid pirates but because around Africa is the best route. The cost of providing a highly trained, armed security detail to protect a 2-million-barrel very large crude carrier from pirates is roughly three cents per barrel—an insignificant amount to guarantee that the ship will not be hijacked.[1] U.S. citizens are not at risk, and U.S. foreign commerce is not threatened.

The U.S. role as defender of order in the maritime global commons needs to be evaluated, as President Obama has implied. With constrained defense budgets, the Powell Doctrine (*14*), influential in the 1990s, again may become the predominant analytical framework. The doctrine specifies that a compelling national interest justifies the use of force; if justified, the force must be sufficient to ensure victory, with a clear end state and exit strategy.

[1] Author's calculations based on experience placing armed security on ships trading in that area.

Image courtesy of the Naval Historical Foundation

This painting, circa 1810, depicts Stephen Decatur in combat with Barbary pirates during the 1804 bombardment of Tripoli. The economic significance of piracy for the United States was far greater in the 19th century than it is today.

If the U.S. role in securing the global commons from Somali piracy does not meet the national interest test to justify the use of U.S. armed forces, the U.S. should withdraw its forces and leave the matter to those most affected—Europe, Asia, and Africa. If vital U.S. national interest is served in using U.S. armed forces, then insufficient force is being applied and with no evident exit strategy, contrary to the Powell Doctrine. If national interest is at stake, then U.S. policy is inadequate and incoherent.

Cost of Piracy

The cost of piracy is difficult to calculate, and estimates are exaggerated. The costs are self-inflicted and have different impacts on different constituencies. The cost is high for people in East Africa, including landlocked countries like Uganda that depend on East African ports. The cost approaches zero for the United States, because foreign commerce has not been affected.

The cost of piracy in terms of ransoms paid is dwarfed by the money made on the piracy business—not by pirates, but by piracy conference organizers and purveyors of antipiracy gizmos. Piracy affects the security of U.S. global supply chains by distracting attention and resources away from more immediate and consequential threats.

Twin Challenges

The international trading system is more complicated than most appreciate, it is multimodal in ways not generally understood, and it behaves according to complex system and network dynamics that cannot be tracked through linear cause-and-effect analyses. The U.S. way of life is not possible without the international trading system, but the system is easy to damage unintentionally.

Policy actions have economic and security consequences that few have yet considered—complex systems can be damaged from a distance. U.S. national security depends on the smooth flow of commerce, but this dependence is not well understood or appreciated. The United States faces twin challenges in maritime security—bad guys and bad policy—and must be vigilant against both.

References

1. *Port Security War Game: Implications for U.S. Supply Chains*. Booz Allen Hamilton, 2003. www.boozallen.com/media/file/128648.pdf.
2. *Secure Trade and 100% Scanning of Containers*. European Commission, February 2010. http://blog.heritage.org/wp-content/uploads/DTS15FEB2010.pdf.
3. *The Economic Effects of 9/11: A Retrospective Analysis*. Congressional Research Service, Sept. 27, 2002. www.fas.org/irp/crs/RL31617.pdf.
4. *Trade in Services and Development Implications*. Commission on Trade in Goods and Services and Commodities, United Nations Conference on Trade and Development. www.unctad.org/sections/wcmu/docs/statement_0103_c1_en.pdf.
5. *Global Navigation Space Systems: Reliance and Vulnerabilities*. Royal Academy of Engineering, United Kingdom, March 2011. www.raeng.org.uk/news/publications/list/reports/RAoE_Global_Navigation_Systems_Report.pdf.
6. *Global Positioning System: Challenges in Sustaining and Upgrading Capabilities Persist*. U.S. Government Accountability Office, September 2010. www.gao.gov/new.items/d10636.pdf.
7. *U.S. Fossil Fuel Resources: Terminology, Reporting, and Summary*. Congressional Research Service, Nov. 30, 2010. http://epw.senate.gov/public/index.cfm?FuseAction=Files.view&FileStore_id=04212e22-c1b3-41f2-b0ba-0da5eaead952.
8. *Independent Statistics and Analysis: Nuclear and Uranium*. U.S. Energy Information Association. www.eia.doe.gov/nuclear/.
9. China Noses Ahead as Top Goods Producer. *Financial Times,* March 13, 2011. www.ft.com/cms/s/0/002fd8f0-4d96-11e0-85e4-00144feab49a,dwp_uuid=9c33700c-4c86-11da-89df-0000779e2340.html#axzz1JbxxLQ4b.
10. *Shopfloor.* National Association of Manufacturers, March 14, 2011. http://shopfloor.org/2011/03/u-s-manufacturing-remains-worlds-largest/18756.
11. Maritime Statistics. U.S. Maritime Administration. www.marad.dot.gov/library_landing_page/data_and_statistics/Data_and_Statistics.htm.
12. www.supplychainbrain.com/content/home/single-article-page/article/congressman-says-tiny-portion-of-american-cargo-carried-by-us-flag-ships-is-security-risk/.
13. Carmel, S. M. The Big Myth of Somali Piracy. *U.S. Naval Institute Proceedings Magazine*, Vol. 136, No. 12, December 2010. http://www.usni.org/magazines/proceedings/2010-12/big-myth-somali-pirates.
14. Preble, C. Weinberger-Powell Doctrine R.I.P. *Cato@Liberty*, March 21, 2011. www.cato-at-liberty.org/weinbergerpowell-doctrine-r-i-p/.

CALENDAR

TRB Meetings 2011

August

22–25 Transportation Hazards and Security Summit
Irvine, California

29–Sept. 1 Rethinking Energy and Climate Strategies for Transportation (invitation only)
Pacific Grove, California

30–Sept. 1 Emerging Issues in Safe and Sustainable Mobility for Older People
Washington, D.C., area

September

7–8 Performance Measures for Transportation and Livability*
Austin, Texas

13–16 Smart Rivers 2011: Systems Thinking*
New Orleans, Louisiana

14–16 3rd International Conference on Road Safety and Simulation
Indianapolis, Indiana

October

2–6 7th World Congress on Joints, Bearings, and Seismic Systems for Concrete Structures*
Las Vegas, Nevada

10–12 European Transport Conference*
Glasgow, Scotland

12–13 Fatigue in Transit Operations: A Symposium
Washington, D.C.

16–20 World Congress on Intelligent Transport Systems*
Orlando, Florida
Richard Pain

25–27 Using Census Data for Transportation Applications Conference
Irvine, California

November

2–3 Improving Transportation Safety Programs Through University–Agency Partnerships Conference
Washington, D.C.

7–9 2nd Road Dust Best Management Practices Conference*
Las Vegas, Nevada

15–19 8th International Conference on Managing Pavement Assets*
Santiago, Chile

December

5–7 Strategies for Meeting Critical Data Needs for Decision Making in State and Metropolitan Transportation Agencies (invitation only)
Irvine, California

7–10 1st Conference of the Transportation Research Group of India
Bangalore, India

2012

January

22–26 TRB 91st Annual Meeting
Washington, D.C.
www.TRB.org/AnnualMeeting

April

16–18 9th National Conference on Asset Management
San Diego, California

17–19 Joint Rail Conference: Technology to Advance the Future of Rail Transport*
Philadelphia, Pennsylvania

30–May 3 International Conference on Winter Maintenance and Surface Transportation Weather
Coralville, Iowa

May

20–25 14th International Conference on Alkali–Aggregate Reactions
Austin, Texas

22–24 14th International HOV–HOT and Managed Lanes Conference
Oakland, California

23–25 International Society for Asphalt Pavements Symposium on Heavy-Duty Pavements and Bridge Deck Pavements*
Nanjing, China

Additional information on TRB meetings, including calls for abstracts, meeting registration, and hotel reservations, is available at www.TRB.org/calendar. To reach the TRB staff contacts, telephone 202-334-2934, fax 202-334-2003, or e-mail TRBMeetings@nas.edu. Meetings listed without a TRB staff contact have direct links from the TRB calendar web page.

*TRB is cosponsor of the meeting.

Conrad Ruppert, Jr.

Amtrak

The railroad career of Conrad Ruppert, Jr., had its beginnings in his childhood—a Lionel train set and later a Tyco HO train layout in his family's basement. Ruppert also remembers riding the Hudson Line from Poughkeepsie, New York, into Manhattan, and admiring the city's many structures and buildings—especially Grand Central Terminal. Led by an interest in architecture, he enrolled in a joint architecture and engineering program at Princeton University; he graduated with a bachelor's degree in civil engineering in 1977. Following his senior year, Ruppert accepted the position of junior engineer with Amtrak, which recently had taken over the Northeast Corridor. In the 34 years since, his assignments for the corporation have been in both the field and the office, covering railway track engineering, maintenance operations, and track research.

"It is only through persistent research that we can better understand the dynamic load environment that the railroad infrastructure is exposed to and how we can improve the performance of the infrastructure to withstand those loads in a safe and economical manner."

"Working first in the New York Division, where I was directly involved in the day-to-day maintenance and renewal of the track infrastructure, I began to understand the railroad from the ground up," Ruppert recalls. Among his many projects was the supervision of the renewal of the track structure through the tunnels that go into New York City under the Hudson River.

During these assignments, Ruppert frequently asked the question, "Why do we do things that way?" and often received the answer, "Because we've always done it that way." He observes that, for an industry with a history of more than 200 years, "'always' seemed an awfully long time. I thought there might be an opportunity for change, for daring to do it differently." He adds that research for new ways to do things should always be grounded in reliable, tested methods, however.

Ruppert worked on the New York Division as assistant track supervisor, project engineer, and staff engineer before moving to Philadelphia, Pennsylvania, to join the engineering department's technical staff. There he directed engineering studies and track designs to increase speeds and improve ride quality in the Northeast Corridor; implemented new track surfacing technologies; and led research to improve the performance of track substructure and concrete ties. After 17 years in Philadelphia, he relocated to New England as division engineer. He directed construction and maintenance activities for all engineering disciplines on the New England Division high-speed corridor between New Haven, Connecticut, and Boston, Massachusetts and later helped develop Amtrak's engineering asset management and work management systems. He received a master's engineering degree in technology management from the University of Pennsylvania in 1999.

In the mid-1990s, Ruppert became involved in the rail research community, first through a joint effort on track transitions with Arnold Kerr of the University of Delaware and then through a track substructure study with Ernest Selig of the University of Massachusetts, Amherst. In 1998, Ruppert joined the TRB Railway Maintenance Committee, which he chaired from 2004 to 2010 and still serves. "I was never satisfied with the answers to my question of 'why do we do it that way'; the TRB community provided a forum that combined the practical and the theoretical," he comments. He is a member of the Transportation Safety IDEA Program Committee and a past member of the Rail Group and the Railroad Track Structure System Design Committee.

Ruppert returned to the Philadelphia staff in 2007 as assistant deputy chief engineer–track, responsible for track design, field surveying, track standards and specifications, and several information systems development projects. Current projects include the development of a compliance management system for Northeast Corridor track inspections and preliminary engineering design efforts for two new tunnels under the Hudson River into Penn Station in New York.

Railway research is hard work, Ruppert notes; his early experience in the field has proved invaluable as his career has progressed. "It is only through persistent research that we can better understand the dynamic load environment that the railroad infrastructure is exposed to and how we can improve the performance of the infrastructure to withstand those loads in a safe and economical manner," he observes.

Ruppert also mentors new track engineers via Amtrak's Management Associate Program. He advises young rail researchers and engineers, "Never be afraid to ask the question, 'Why?' and always be willing to learn from those who have come before."

Martha Grabowski

Le Moyne College and Rensselaer Polytechnic Institute

Filling several leadership roles at Le Moyne College in Syracuse, New York, Martha Grabowski is professor and chair of the business administration department, McDevitt Associate Chair in Information Systems, and director of the information systems program; in addition, she serves as research professor at her alma mater, Rensselaer Polytechnic Institute (RPI) in Troy, New York. After earning a bachelor's degree in nautical science from the U.S. Merchant Marine Academy in 1979, she received a master of sciences degree in industrial engineering, a master's degree in business administration, and a Ph.D. in management and information systems from RPI.

Grabowski's teaching, consulting, and research encompass a wide range of topics—the impact of technology in safety-critical systems, human factors in systems design, risk analysis and mitigation in large-scale systems, and human and organizational error in high-consequence settings. "Young investigators and those new to large-scale systems research could not be launching their careers at a more exciting time," she notes.

"Basic and applied research is the essential elixir of a vibrant economy and a sustainable world."

Grabowski currently is leading a research project that explores the role of social media in emergency response—particularly the response to the March 2011 earthquakes in Sendai, Japan. The project team will use various media to construct a timeline of warnings during the quake and will map the data to the social processes in theoretical decision making and to the informal network used by the public in response to the warnings. Models will analyze informal and formal networks and link them to response behavior. Multidisciplinary methods and interdisciplinary studies are essential to breakthroughs in research, Grabowski observes: "The blend of traditional methodologies and new technology, and of disparate disciplines and cultures that approach the same problem from different perspectives, can produce a grand conversation worthy of the grand challenges for new investigators to address."

Grabowski's past projects include the development of a business process analysis template for next-generation short-haul trucking; an 8-year study of leading indicators of risk in marine transportation; a decade-long project developing embedded intelligent ship-piloting systems for merchant and naval vessels; and several major maritime risk assessment projects in Washington's Puget Sound, Alaska's Prince William Sound, the lower Mississippi River, and the Port of Houston. Research collaboration and innovation are indispensable in these projects, and when new researchers consider future challenges, she reflects: "Basic and applied research is the essential elixir of a vibrant economy and a sustainable world. Transportation research plays a critical role in providing solutions to many problems, and advances in energy, platforms, vehicles, critical infrastructure, networks, engineering design, human–technology interaction, and materials—and in understanding how large-scale, complex systems behave and interact—will have much to do with the quality and equity of life on our planet in the years to come."

A retired lieutenant commander in the U.S. Naval Reserve, Grabowski began working at Le Moyne in 1987 and at RPI in 1988. At Le Moyne, Grabowski is helping launch a School of Management, as well as new programs in health information systems, government contract management, and a bachelor's–master's degree program in information systems.

Grabowski recently chaired the Committee on Naval Engineering in the 21st Century, which produced a TRB–Marine Board policy study report reviewing the future of naval engineering for the U.S. Navy Office of Naval Research. She first joined the Marine Board in 1992; as chair from 2006 to 2008, she also served on the TRB Executive Committee. Grabowski is a member of the TRB Marine Safety and Human Factors Committee and has worked on National Research Council studies on topics that include tsunami preparedness and warning systems and shipboard display of automatic identification systems information.

The breadth and complexity of issues in transportation make this a promising time for new researchers, Grabowski muses. She counsels young researchers to expand the impact of their findings by "periodically refreshing their intellectual and personal worlds, listening well and reflecting often, collaborating with other great minds in the service of others, maintaining a healthy sense of humor, and passing on their wonderful gifts and talents—especially those that have benefited from the care and hand of a thoughtful mentor."

In 2003, Grabowski was named a lifetime National Associate of the National Academies in recognition of her extraordinary service. She received a Navy Achievement Medal in 1988. She is a member of the American Bureau of Shipping, the Association for Information Systems, the Institute for Operations Research and the Management Sciences, and the Decision Sciences Institute.

NEWS BRIEFS

Mobile Phones Yield Traveler Advisory Data

By SEAN J. BARBEAU, NEVINE L. GEORGGI, and PHILIP L. WINTERS
Center for University Transportation Research, University of South Florida

PHOTO: FLORIDA DOT

The FL511 Traffic Management Center in Palm Beach, Florida. FL511 also has launched an iPhone application.

To promote safety and better serve the public, researchers at the University of South Florida have designed an improved traveler information mobile application to feature pertinent, timely alerts filtered and customized to real-time and historical individual travel behavior. Although Florida 511 (FL511) features live, extensive coverage of travel conditions on the Interstates, at the time of the project's end date, the website had not directly integrated public transportation information. FL511's subscription-based road and traffic condition alerts—delivered via text message, e-mail, or telephone call—are numerous, however. As a result, useful information often is lost in an avalanche of irrelevant alerts for roads the traveler does not use; accessing messages while driving can be hazardous. The researchers deployed TRAC-IT, a software system that collects data about a user's travel behavior and delivers real-time, location-based services via Geographic Positioning System (GPS)–enabled mobile phones, allowing the FL511 system to generate and deliver alerts more efficiently.

The project had three objectives: to increase the likelihood that alerts will influence a traveler's mode choice, departure time, route, or decision to take the trip; to provide real-time transit information via cell phones to current and potential transit riders; and to devise a method for sending pertinent text message alerts to a user's cell phone in a way that minimizes driver distraction.

The current travel alerts are static subscriptions that do not filter for the user's actual travel time and location or for past travel behavior. To determine how many e-mail and text messages are sent by FL511, the research team subscribed to alerts for I-75 and I-275 in the Tampa Bay area. From July 15, 2009, to December 31, 2010, a single user received 6,851 e-mails—60 or more e-mails per day—and even more text messages. Researchers were able to reduce the number of irrelevant alerts by applying path prediction technology, which creates a profile of a traveler's typical daily movements. TRAC-IT's mobile system enables GPS data collection and user notification; the server hosts spatial databases and creates real-time spatial predictions. Because the program does not depend on road network data, it can build a user travel history for transit riders, pedestrians, and bicyclists.

Researchers designed a clustering algorithm that uses location data from GPS-enabled mobile phones to determine a traveler's points of interest (POIs). The algorithm can process large volumes of GPS data efficiently and can signal areas of frequent traffic congestion or delay. Predictions are based on POIs, as well as on trip segmentation, driver destinations, and departure times.

Researchers also integrated transit estimated arrival data from Hillsborough Area Regional Transit's automatic vehicle location system with FL511 messages delivered to a single mobile interface. In addition, a prototype application, traffic text-to-speech, delivered traffic information only when the user was traveling below the established speed threshold or had stopped moving. Although GPS-enabled cell phones can support the tracking and prediction service, the cost on battery life is significant—especially on smart phones. The researchers also have created software that reduces the negative impact of location-based services on battery life significantly.

The team identified additional research needs before full-scale deployment; future research could extend TRAC-IT's use with smart phone platforms and could allow FL511 to integrate more real-time transit information and deploy more project technologies for improved personalized traffic information.

For more information, contact Sean Barbeau, CUTR Research Associate, at 813-974-7208 or Barbeau@cutr.usf.edu; Amy Datz, Florida DOT Project Manager, at 850-414-4239 or Amy.Datz@dot.state.fl.us; or visit the project website at www.nctr.usf.edu/2011/03/dynamic-travel-information-personalized-and-delivered-to-your-cell-phone-2.

TRB HIGHLIGHTS

States Implement SHRP 2 Research

Two dozen states are involved in Second Strategic Highway Research Program (SHRP 2) activities—including the naturalistic driving study, workshops, pilot tests of SHRP 2 products, field tests, focus groups, and demonstrations. Projects include the pilot testing in Jacksonville, Florida, of an advanced travel-demand model that integrates traveler choice and network conditions; pilot tests of an incident management training course developed in a SHRP 2 project; a naturalistic driving study conducted in Florida, Indiana, North Carolina, New York, Pennsylvania, and Washington State; the design and replacement of a bridge near Council Bluffs, Iowa, using accelerated bridge construction; and more. SHRP 2 focus areas and the states involved in projects are as follows:

- Capacity projects to reduce congestion: California, Colorado, Florida, Minnesota, Oregon, Washington, and West Virginia;
- Reliability projects to reduce congestion and improve travel time reliability: Georgia and Indiana;
- Safety projects to study driving behavior: Florida, Indiana, New York, North Carolina, Pennsylvania, and Washington State; and
- Renewal projects to speed project delivery: Arkansas, California, Delaware, Florida, Georgia, Illinois, Iowa, Kansas, Maine, Michigan, Minnesota, Missouri, Oklahoma, New Jersey, New York, Texas, and Virginia.

PHOTO: MANNY ASCHEMEYER

HONORING SAFE HARBORS—Eunice Ratcliff (*second from right*) received the Harbor Safety Committee of the Year Award, presented to the Waterways Association of Pittsburgh, Pennsylvania, with Jeff High, Northrop Grumman (*left*); Rear Admiral Roy Nash, U.S. Coast Guard (*second from left*); and Dana Goward, U.S. Coast Guard (*right*). The Joint Harbor Safety and Area Maritime Security Committees Conference, June 7–9, 2011, in Houston, Texas, was sponsored by the TRB Marine Board and the U.S. Coast Guard and was hosted by the Houston–Galveston Navigation Safety Advisory Committee, the Southeast Texas Waterways Advisory Council, the Houston Area Maritime Security Committee, and the Sabine–Neches Area Maritime Security Committee. With a record attendance, the conference featured addresses from Admiral Robert J. Papp, Commandant, U.S. Coast Guard, and Rear Admiral Harris Sinclair, Director, U.S. Navy Irregular Warfare Office.

COOPERATIVE RESEARCH PROGRAMS NEWS

Long-Term Field Performance of Warm-Mix Asphalt Technologies

The benefits of warm-mix asphalt (WMA) technology include lower energy demand during production and construction, reduced emissions at plants and pavers, and increased allowable haul distances. But lower production temperatures and water injection have raised concerns about rutting and moisture susceptibility of WMA pavement. Definitive information is needed on the material and engineering properties and long-term performance of WMA pavements.

Washington State University has received a $900,000, 63-month contract [National Cooperative Highway Research Program (NCHRP) Project 09-49A, FY 2010] to identify the material and engineering properties that determine WMA pavement performance and to recommend best practices for the use of WMA technologies.

For more information, contact Ed Harrigan, TRB, 202-334-3232, eharriga@nas.edu.

Self-Consolidating Concrete for Cast-in-Place Bridge Components

Self-consolidating concrete is a specially proportioned hydraulic cement concrete that enables fresh concrete to flow easily into forms and around steel reinforcement without segregation. Because this type of concrete allows for faster production, increased safety, reduced labor needs, and lower noise levels at manufacturing plants, its use in precast, prestressed bridge elements is growing. Cast-in-place, self-consolidating concrete rarely has been used in bridge construction, however; design and construction guidelines are lacking. Research documented in NCHRP Report 628, *Self-Consolidating Concrete for Precast, Prestressed Concrete Bridge Elements*, focused on the application of this concrete in precast, prestressed bridge elements; however, its use in cast-in-place applications requires the consideration of outside conditions.

The University of Nebraska–Lincoln has been awarded a $499,831, 36-month contract (NCHRP Project 18-16, FY 2011) to develop guidelines for the use of self-consolidating concrete in cast-in-place highway bridge components and to recommend changes to the American Association of State Highway and Transportation Officials' (AASHTO) *Load and Resistance Factor Design (LRFD) Bridge Design and Construction Specifications*.

For further information, contact Amir N. Hanna, TRB, 202-334-1432, ahanna@nas.edu.

(continued on next page)

TRB HIGHLIGHTS

IN MEMORIAM

Roy C. Edgerton, 1914–2011

Roy C. Edgerton, TRB's first Technical Activities Division director, died June 12, 2011, in Arlington, Virginia. He was 97. Edgerton was a 1978 recipient of the TRB Distinguished Service Award (renamed the W. N. Carey, Jr., Distinguished Service Award in 1987).

Born in Louisiana, Edgerton grew up in Wyoming and Washington State before moving to Klamath Falls, Oregon, where he finished high school. In 1934, he enrolled at Oregon State College (now Oregon State University). Edgerton left college to work for the Oregon Highway Department and later served as a field artillery officer with the U.S. Army in Europe during World War II. He received a Purple Heart in 1945 and continued in the Army Reserves, retiring as a colonel in 1974.

Edgerton received a bachelor's degree in civil engineering in 1948 and resumed work at the Oregon Highway Department, eventually directing its research division. In 1962, Edgerton joined TRB—then the Highway Research Board—as assistant engineer and became Technical Activities Director in 1967. He coordinated TRB's field visits, committee activities, Annual Meeting programs, conferences, and special assignments. Edgerton's award citation noted his "patient and persuasive application of effective principles of management" and commended his leadership for bringing eight independent departments together into a smoothly functioning division. He retired in 1979.

Edgerton's wife, Shirley, died in 2005. He is survived by his niece, Lorraine Brooks, and his nephew, Robert Bekker.

PHOTO: RISDON PHOTOGRAPHY

Edgerton acknowledges applause at the 2009 TRB Annual Meeting's Chairman's Luncheon.

COOPERATIVE RESEARCH PROGRAMS NEWS (*continued*)

Treatment of Airport Stormwater After Deicing

U.S. airports face increased regulatory and technical challenges in dealing with the runoff from deicing operations; glycol-based aircraft deicing and anti-icing fluids are often detected in the effluent. Requirements for the handling and discharging of millions of gallons of runoff stormwater and wastewater vary among states. Although guidelines being developed by the Environmental Protection Agency likely will standardize effluent limits and collection efficiency requirements, airports will have to evaluate treatment options in implementing the new regulations. Several airports have applied biological treatments to deicing stormwater runoff, but the effects of cold water temperatures on system performance and the treatment's efficiency have not been sufficiently documented.

PHOTO: DENVER INTERNATIONAL AIRPORT

An aircraft is deiced just before takeoff.

Gresham, Smith, and Partners have received a $600,000, 20-month contract (ACRP Project 02-29, FY 2011) to identify available and emerging technologies for treating runoff from airport deicing activities, evaluate the performance of available technologies, and provide guidance for airports on treating runoff.

For further information, contact Joseph D. Navarrete, TRB, 202-334-1649, jnavarrete@nas.edu.

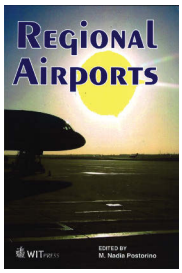
Recommended Tunnel Design and Construction Specifications

The section of AASHTO's *LRFD Bridge Design Specifications* that examines buried structures and tunnel liners provides minimal information on the design and construction of highway tunnels. Although AASHTO adopted the Federal Highway Administration's *Technical Manual for Design and Construction of Road Tunnels—Civil Elements*, design and construction specifications for tunnels are needed.

PB Americas, Inc., has received a $699,979, 36-month contract (NCHRP Project 12-89, FY 2011) to develop stand-alone design and construction specifications for highway tunnel systems that address safety and operations, maintenance, and inspection.

For further information, contact Waseem Dekelbab, TRB, 202-334-1409, wdekelbab@nas.edu.

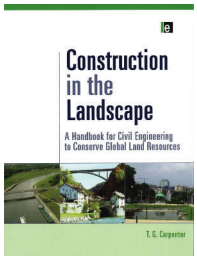
Regional Airports



M. Nadio Postorino, Editor. WIT Press, 2011; 138 pp.; $118; 978-1-84564-570-0.

With congestion at main hubs and demand for air transportation increasing, the role of regional airports—as origins, destinations, and feeders—is growing. The papers in this volume examine the optimization of air networks within the larger context of transportation and reevaluate the role of regional airports in a sustainable air transportation system. Papers address issues that include airport–airline relationships, environmental management, economic and social profitability, the accessibility of mountain areas, the design of religious facilities, a sustainable logistics platform, and demand for high-speed rail services in dense air transportation corridors.

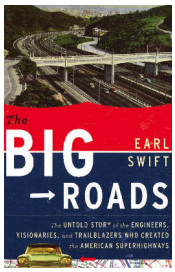
Construction in the Landscape: A Handbook for Civil Engineering to Conserve Global Land Resources



T. G. Carpenter. Earthscan, 2011; 336 pp.; $140; 978-1-84407-923-0.

Carpenter presents a global view of construction's impact on the land and landscape, considering the economic and social needs of different areas as well as their supply of natural resources. Land resources and the effects of construction are examined, along with specific forms of civil engineering, including landform adaptation, coastal construction, transportation infrastructure, bridges, and power stations. The author also delves into construction and land use planning in different geographical areas—from rural to urban and suburban—and investigates sustainable, enduring land arrangements.

The Big Roads



Earl Swift. Houghton Mifflin Harcourt, 2011; 384 pp.; $27; 978-0-618-81241-7.

The Big Roads traces the history of the highways that have traversed the United States since the 1950s. In examining the reverberating effects of the U.S. Interstate Highway System, Swift tells the stories of the architects of American's highways—from Carl Fisher, an influential figure in the building of both the Indianapolis Motor Speedway and the Lincoln Highway, to former Bureau of Public Roads chief Thomas MacDonald, who conceived of a network of interstate highways in the 1920s. The views of citizens affected by the construction of roadways and of critics of the highway system also are examined, including historian Lewis Mumford, who questioned America's growing dependence on the automobile, and activist Joe Wiles, who opposed development that would alter his community.

The books in this section are not TRB publications. To order, contact the publisher listed.

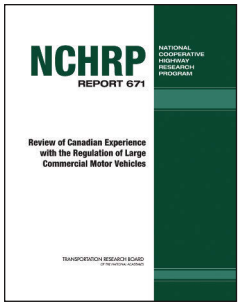
TRB PUBLICATIONS

Review of Canadian Experience with the Regulation of Large Commercial Motor Vehicles
NCHRP Report 671

Canada's process for standardizing size and weight regulations for heavy trucks provides insights for application in the United States. The authors summarize the Canadian framework for truck size and weight regulation and describe efforts to achieve greater uniformity. The lessons can help freight regulators in the United States, who often face jurisdictional challenges in developing and implementing rules for truck configurations that can operate nationwide without compromising safety or creating excessive impacts on roadway pavements.

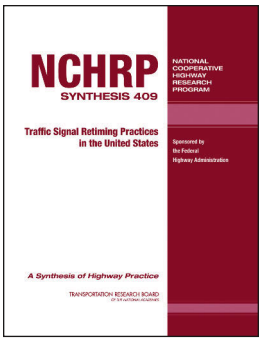
2010; 124 pp.; TRB affiliates, $41.25; nonaffiliates, $55. Subscriber categories: highways; freight transportation; law; policy; vehicles and equipment.

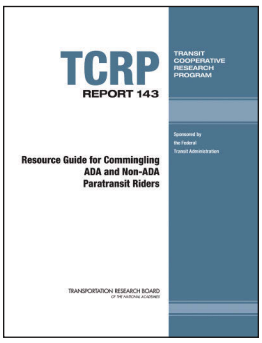
Roundabouts: An Informational Guide—Second Edition
NCHRP Report 672



In the United States, roundabouts increasingly are being used as a form of intersection control. Selecting and designing a roundabout requires a balance between transportation-oriented objectives, such as safety, operational performance, and accessibility, with other concerns, such as economics, land use, aesthetics, and the environment. First published in 2000 by the Federal Highway Administration, this guide draws its findings from established and emerging U.S. practices and from recent research. Through planning and design guidance, operational and safety performance evaluations, construction and maintenance information, and the examination of many potential roundabout applications, this report

BOOK SHELF





TRB PUBLICATIONS *(continued)*

encourages independent designs and techniques for various situations and emphasizes a performance-based evaluation of the designs.

2010; 396 pp.; TRB affiliates, $64.50; nonaffiliates, $86. Subscriber categories: highways; design.

Development of Levels of Service for the Interstate Highway System

NCHRP Report 677

A major national investment, the Interstate Highway System is vital to the nation's economy. Although the system is increasingly essential to global production and distribution systems, its assets are owned and managed by the states. The specific measures that define levels of service can vary from one state to another; therefore, a consistent framework and measurement for Interstate Highway System levels of service can help state transportation agencies maintain and manage their assets. This report examines an approach, based on levels of service, to create a description of Interstate highway asset performance.

2010; 40 pp.; TRB affiliates, $36.75; nonaffiliates, $49. Subscriber categories: administration and management; economics; highways; maintenance and preservation; planning and forecasting; policy.

Traffic Signal Retiming Practices in the United States

NCHRP Synthesis 409

Traffic signals that are not timed to coordinate with vehicular traffic can cause travel delays and increase accident rates, pollution, and fuel consumption. Although many studies have shown that retiming traffic signals is a cost-effective way to use resources, few agencies have developed regular programs to retime the signals in their jurisdictions. New approaches to signal retiming can improve the quantity and quality of the traffic signal data collected and can streamline the use of new and existing resources for transportation agencies. This synthesis, which comprises a literature review, findings from four transit agency surveys, and a series of project case studies, explores the processes to develop, install, verify, fine-tune, and evaluate signal timing plans.

2010; 80 pp.; TRB affiliates, $37.50; nonaffiliates, $50. Subscriber categories: highways; operations and traffic management; safety and human factors.

Freight Transportation Surveys

NCHRP Synthesis 410

From classified traffic counts and travel time studies to comprehensive commodity flow and origin–destination surveys, information on freight movement is essential in promoting economic efficiency and development. This synthesis gathers information from a literature review and a survey of state departments of transportation, selected metropolitan planning organizations, marine and airport authorities, academics, and commercial freight data purveyors. The surveys detail crosscutting issues, the use of intelligent transportation system technologies and the Commodity Flow Survey; also covered are survey costs and a comparison of survey types.

2011; 78 pp.; TRB affiliates, $39; nonaffiliates, $52. Subscriber categories: highways; motor carriers; planning and forecasting; railroads; terminals and facilities.

Microsurfacing

NCHRP Synthesis 411

Microsurfacing—a polymer-modified cold-mix surface treatment—can remedy many problems on highways. Effective practices used by transportation agencies—such as microsurfacing project selection, design, contracting, equipment, construction, and performance measures—are explored in this volume. Included are a literature review, findings from a survey of maintenance engineers at transportation agencies in the United States and Canada, an evaluation of state and national microsurfacing specifications, and case studies of six microsurfacing projects in North America.

2010; 115 pp.; TRB affiliates, $41.25 ; nonaffiliates, $55. Subscriber categories: highways; maintenance and preservation; materials.

Resource Guide for Commingling ADA and Non-ADA Paratransit Riders

TCRP Report 143

Since transit agencies began operating paratransit services under the Americans with Disabilities Act of 1990 (ADA), a key decision has been whether to commingle—that is, transport together—riders who use paratransit services and those who do not. This guide presents a road map to planning for commingled services. The decision-making process is organized into four components: defining the purpose and objectives for commingling riders, identifying capacity and funds, evaluating service compatibility, and considering primary service parameters. The operations decision process focuses on developing policies, procedures, practices, and performance- monitoring strategies. Important lessons are presented from transit agencies that have decided to commingle and from those that have chosen not to commingle their ADA

TRB PUBLICATIONS *(continued)*

and non-ADA riders.

2011; 103 pp.; TRB affiliates, $39.75; nonaffiliates, $53. Subscriber category: public transportation.

Guidebook for Developing and Managing Airport Contracts

ACRP Report 33

This intuitive, accessible guidebook provides a single resource of best practices for developing, soliciting, preparing, administering, and managing airport agreements and contracts. Airline, communication and utility service, common use, ground transportation, and concession agreements for many passenger services are described. An accompanying CD-ROM includes samples of agreements in each area.

2011; 74 pp.; TRB affiliates, $43.50; nonaffiliates, $58. Subscriber categories: aviation; finance; law; terminals and facilities.

Freight-Demand Modeling to Support Public-Sector Decision Making

NCFRP Report 8

Although the private sector is mostly responsible for developing and managing the nation's freight-flow system, public agencies often make investment and policy decisions that can affect the flows. To understand the shifts of traffic in the nation's freight flows, many state, regional, and federal agencies have begun to create freight demand models; however, these agencies need more capability to analyze freight demand. The authors explore possible ways to improve freight demand models and other analysis tools.

2010; 58 pp.; TRB affiliates, $33.75; nonaffiliates, $45. Subscriber categories: data and information technology; freight transportation; marine transportation; motor carriers; planning and forecasting; policy; railroads.

Planning 2010

Transportation Research Record 2174

The papers in this volume explore wide-area congestion and incident monitoring, the estimation of a state funding shortfall for transportation infrastructure, a microsimulation analysis of paratransit accessibility, using intelligent transportation system technologies to improve shuttle ridership, prioritizing transportation projects, the ConnectOregon multimodal funding program, ramp metering and urban sprawl, commuting and the jobs–housing balance, residential property values and the built environment, and more.

2010; 155 pp.; TRB affiliates, $51; nonaffiliates, $68. Subscriber categories: highways; public transportation; pedestrians and bicyclists; planning and forecasting; policy; economics; environment; data and information technology.

Travel Forecasting 2010, Vol. 1

Transportation Research Record 2175

Mixed logit models; multiagent transport simulations; real-time, short-term traffic speed forecasting; transferability of mode–destination models; a patronage ramp-up analysis model; calibrating activity-based models with origin–destination information; multiple objectives in travel demand modeling; and other travel forecasting topics are covered in this volume.

2010; 147 pp.; TRB affiliates, $51; nonaffiliates, $68. Subscriber categories: highways; public transportation; pedestrians and bicyclists; planning and forecasting; passenger transportation; economics; environment; data and information technology.

Travel Forecasting 2010, Vol. 2

Transportation Research Record 2176

Authors present research on topics that include a large-scale GPS-based household travel survey, integrating transportation and land use, calibration and validation of a hybrid accessibility-based model, estimating price elasticities of ferry demand, using an intelligent transportation system as an evaluation tool in a regional demand modeling environment, and an accelerated procedure for multiclass highway traffic assignment in a statewide transportation model.

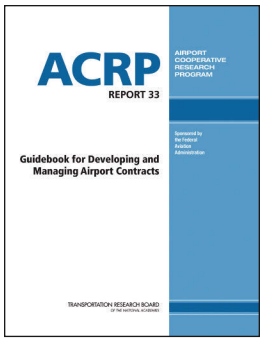
2010; 91 pp.; TRB affiliates, $42.75; nonaffiliates, $57. Subscriber categories: highways; public transportation; pedestrians and bicyclists; planning and forecasting; passenger transportation; economics; environment; data and information technology.

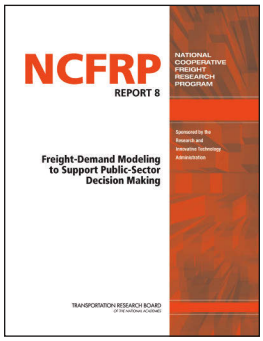
Aviation 2010

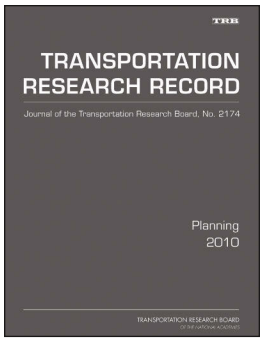
Transportation Research Record 2177

The 16 papers in this volume examine a benefit–cost analysis of airport improvements, the impact of

The TRR Journal Online website provides electronic access to the full text of more than 11,000 peer-reviewed papers that have been published as part of the Transportation Research Record: Journal of the Transportation Research Board *(TRR Journal) series since 1996. The site includes the latest in search technologies and is updated as new TRR Journal papers become available. To explore the TRR Online service, visit www.TRB.org/TRROnline.*







BOOK SHELF

TRB PUBLICATIONS *(continued)*

airport noise on property values, aviation emissions mitigation, the sensitivity of airline schedules to airport congestion pricing, the policy implications of airline performance indicators, automated measurement of airport security wait times, using multimodalism to mitigate airport congestion, statistical characteristics of aircraft arrival tracks, the impact of flight delay on air traffic flow, new materials for aircraft arrestor beds, and more.

2010; 140 pp.; TRB affiliates, $44.25; nonaffiliates, $59. Subscriber categories: aviation; railroads; environment; economics; operations and traffic management; security and emergencies; planning and forecasting.

Freeway Operations; Regional Systems Management and Operations; Managed Lanes 2010
Transportation Research Record 2178

Investigated are subjects that include a heuristic ramp-metering coordination strategy, queue management for metered freeway on-ramps, freeway travel time prediction under incident conditions, freeway traffic speed during breakdown and recovery periods, algorithms for the systematic tracking of traffic congestion patterns on freeways, proactive incident management and strategic planning, models of concurrent-flow lane violations, an investigation of single-occupant travelers in high-occupancy vehicle lanes, and a dynamic toll concept to assess the feasibility of high-occupancy vehicle lanes.

2010; 176 pp.; TRB affiliates, $54; nonaffiliates, $72. Subscriber categories: highways; operations and traffic management; safety and human factors; finance.

Bituminous Materials and Mixtures 2010, Vol. 1
Transportation Research Record 2179

The papers in this volume examine topics such as recycled concrete aggregate affected by an alkali–silica reaction; the construction, rehabilitation, and material alternatives for flexible pavement; measuring low-temperature properties of asphalt binders; the influence of aging temperature on rheological and chemical properties of asphalt binders; polyphosphoric acid modification of asphalt; aggregate retention of chip seals; the use of thixotropy to analyze fatigue and healing characteristics of asphalt binder; and more.

2010; 108 pp.; TRB affiliates, $44.25; nonaffiliates, $59. Subscriber categories: highways; materials; geotechnology; environment.

Bituminous Materials and Mixtures 2010, Vol. 2
Transportation Research Record 2180

Authors present research on fracture characteristics of asphalt mixtures, temperature and shear susceptibility of a nonpetroleum binder, the workability and compactability of warm-mix asphalt, the influence of aggregate blending on asphalt mixture strength, rutting resistance in warm-mix asphalts containing moist aggregate, asphalt mixtures modified with synthetic waxes, crumb rubber–modified asphalt mixtures, a local calibration of the *Mechanistic–Empirical Pavement Design Guide* rutting model, and the bonding properties of bituminous tack coat.

2010; 164 pp.; TRB affiliates, $51; nonaffiliates, $68. Subscriber categories: highways; materials; geotechnology; environment.

Bituminous Materials and Mixtures 2010, Vol. 3
Transportation Research Record 2181

Permanent deformation of asphalt mixtures, a prediction of the mechanical behavior of asphalt mixtures, a new test procedure for evaluating cracking resistance in bituminous mixtures, the effect of thermal stresses on pavement performance, the flow number simple performance test, predictive models for populating the dynamic moduli of long-term pavement performance sections, stiffening mechanisms of asphalt–aggregate mixtures, and the estimate of fatigue shift factors between laboratory tests and field performance are among the topics covered in this volume.

2010; 124 pp.; TRB affiliates, $44.25; nonaffiliates, $59. Subscriber categories: highways; materials; geotechnology; environment.

Highway Safety: Behavior, Management, and Roundabouts
Transportation Research Record 2182

The papers in this volume address subjects such as ways to monitor drinking, technology that assists novice drivers, the driving and crash histories of illegal street racing offenders, seat belt use on school buses, speed enforcement cameras, law enforcement vehicle crashes, automated enforcement for red-light running, travel behavior in aging societies, the willingness of seniors to use an alternative service bus, aggressive driving and safety campaigns, a reward system to encourage safer driving practices, road safety audits, and roundabouts.

2010; 147 pp.; TRB affiliates, $51; nonaffiliates, $68. Subscriber categories: highways; safety and human factors; design; operations and traffic management.

To order TRB titles described in Bookshelf, visit the TRB online Bookstore, at www.TRB.org/bookstore/, or contact the Business Office at 202-334-3213.

INFORMATION FOR CONTRIBUTORS TO

TR NEWS

TR News welcomes the submission of manuscripts for possible publication in the categories listed below. All manuscripts submitted are subject to review by the Editorial Board and other reviewers to determine suitability for *TR News*; authors will be advised of acceptance of articles with or without revision. All manuscripts accepted for publication are subject to editing for conciseness and appropriate language and style. Authors receive a copy of the edited manuscript for review. Original artwork is returned only on request.

FEATURES are timely articles of interest to transportation professionals, including administrators, planners, researchers, and practitioners in government, academia, and industry. Articles are encouraged on innovations and state-of-the-art practices pertaining to transportation research and development in all modes (highways and bridges, public transit, aviation, rail, and others, such as pipelines, bicycles, pedestrians, etc.) and in all subject areas (planning and administration, design, materials and construction, facility maintenance, traffic control, safety, geology, law, environmental concerns, energy, etc.). Manuscripts should be no longer than 3,000 to 4,000 words (12 to 16 double-spaced, typed pages). Authors also should provide appropriate and professionally drawn line drawings, charts, or tables, and glossy, black-and-white, high-quality photographs with corresponding captions. Prospective authors are encouraged to submit a summary or outline of a proposed article for preliminary review.

RESEARCH PAYS OFF highlights research projects, studies, demonstrations, and improved methods or processes that provide innovative, cost-effective solutions to important transportation-related problems in all modes, whether they pertain to improved transport of people and goods or provision of better facilities and equipment that permits such transport. Articles should describe cases in which the application of project findings has resulted in benefits to transportation agencies or to the public, or in which substantial benefits are expected. Articles (approximately 750 to 1,000 words) should delineate the problem, research, and benefits, and be accompanied by one or two illustrations that may improve a reader's understanding of the article.

NEWS BRIEFS are short (100- to 750-word) items of interest and usually are not attributed to an author. They may be either text or photographs or a combination of both. Line drawings, charts, or tables may be used where appropriate. Articles may be related to construction, administration, planning, design, operations, maintenance, research, legal matters, or applications of special interest. Articles involving brand names or names of manufacturers may be determined to be inappropriate; however, no endorsement by TRB is implied when such information appears. Foreign news articles should describe projects or methods that have universal instead of local application.

POINT OF VIEW is an occasional series of authored opinions on current transportation issues. Articles (1,000 to 2,000 words) may be submitted with appropriate, high-quality illustrations, and are subject to review and editing. Readers are also invited to submit comments on published points of view.

CALENDAR covers (*a*) TRB-sponsored conferences, workshops, and symposia, and (*b*) functions sponsored by other agencies of interest to readers. Notices of meetings should be submitted at least 4 to 6 months before the event.

BOOKSHELF announces publications in the transportation field. Abstracts (100 to 200 words) should include title, author, publisher, address at which publication may be obtained, number of pages, price, and ISBN. Publishers are invited to submit copies of new publications for announcement.

LETTERS provide readers with the opportunity to comment on the information and views expressed in published articles, TRB activities, or transportation matters in general. All letters must be signed and contain constructive comments. Letters may be edited for style and space considerations.

SUBMISSION REQUIREMENTS: Manuscripts submitted for possible publication in *TR News* and any correspondence on editorial matters should be sent to the Director, Publications Office, Transportation Research Board, 500 Fifth Street, NW, Washington, DC 20001, telephone 202-334-2972, or e-mail jawan@nas.edu.

◆ All manuscripts should be supplied in 12-point type, double-spaced, in Microsoft Word 6.0 or higher versions, on a CD or as an e-mail attachment.

◆ Submit original artwork if possible. Glossy, high-quality black-and-white photographs, color photographs, and slides are acceptable. Digital continuous-tone images must be submitted as TIFF or JPEG files and must be at least 3 in. by 5 in. with a resolution of 300 dpi or greater. A caption should be supplied for each graphic element.

◆ Use the units of measurement from the research described and provide conversions in parentheses, as appropriate. The International System of Units (SI), the updated version of the metric system, is preferred. In the text, the SI units should be followed, when appropriate, by the U.S. customary equivalent units in parentheses. In figures and tables, the base unit conversions should be provided in a footnote.

NOTE: Authors are responsible for the authenticity of their articles and for obtaining written permissions from publishers or persons who own the copyright to any previously published or copyrighted material used in the articles.