



Protecting America's Ports

by Bruce Taylor, Ph.D., and Pat Kaufman

The recent terrorist attacks in Mumbai, India, brought to the forefront long-standing concerns about the vulnerability of our ports. After Sept. 11, for example, U.S. seaports were closed for several days, an acknowledgment that ships, like airplanes, could also serve as deadly weapons. Coast Guard vessels were immediately dispatched to provide security at all major American ports.¹

Few would dispute that, if terrorists used a cargo container to conceal a weapon of mass destruction and detonated it on arrival at a U.S. port, the impact on global trade and the world economy could be immediate and devastating.

Protecting America's ports against a terrorist threat is daunting because of the sheer size and sprawling nature of the U.S. maritime system and because the United States has no central port authority to oversee security. Approximately 8,000 ships with foreign flags make 51,000 calls on U.S. ports each year. Fully 95 percent of overseas commerce (and

100 percent of foreign oil) comes by ship.² In addition, more than 6.5 million passengers from cruise ships pass through the nation's ports each year, along with approximately 9 million cargo containers — about 26,000 cargo containers a day.³ The complex structure of ports and the port authorities that govern them — including the variation in public and private ownership, the involvement of multiple governmental and private agencies, and the differences in levels and scopes of authority — makes securing U.S. ports a tremendously difficult task.

Because little was known about the nature of anti-terrorist activities in the nation's ports or which security practices might be worthy of further examination and testing, the National Institute of Justice (NIJ) funded the Police Executive Research Forum to identify promising local practices to safeguard America's ports against terrorist attacks.

The researchers used an exploratory or descriptive case study methodology to

analyze interorganizational relationships in port security operations between 2003 and 2006. Because port security practices have not been evaluated, even with non-rigorous methods, they took a basic qualitative approach to learn what we do not know, gain an elementary understanding of the challenges and create a foundation for future research, which the researchers hope will include traditional evaluation methods, such as quantitative surveys and randomized control trials.

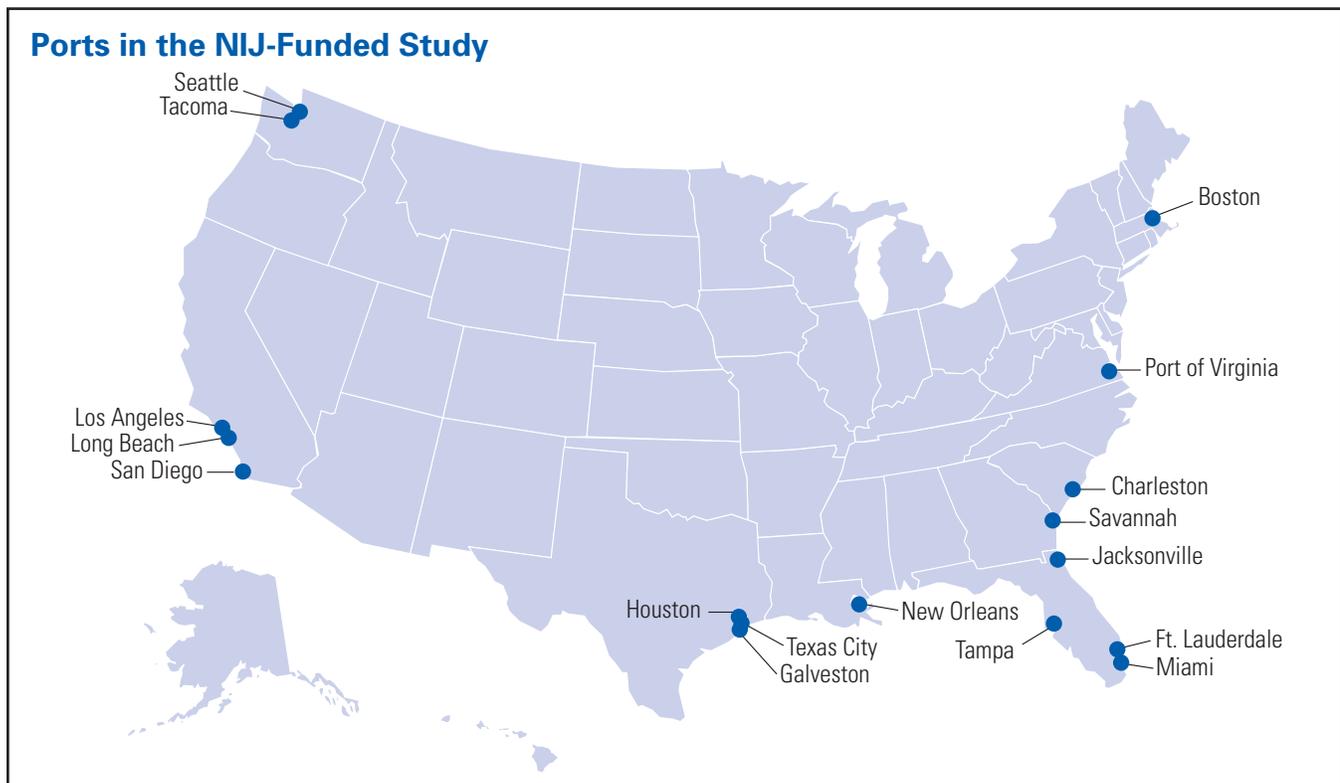
The research team assembled rich descriptions of the problem and context for port security and identified promising practices based on the expert opinion and experience of port personnel. The resulting research offers valuable insights into practices used in a variety of ports. In the future, by building on the findings, researchers will be in a better position to evaluate the effectiveness of the security initiatives.

With the help of an expert advisory board of stakeholders in the port security community, the research team selected 17 ports to study (see “Ports in the NIJ-Funded Study”

below).⁴ These ports represented America’s maritime industry in terms of the variety of vessels, the volume of cargo and passengers, the types of ownership, law enforcement presence, and geographic location. To identify promising security practices, with a particular focus on successful intergovernmental and public-private partnerships, the team met with local, state and federal agency officials who were involved in managing each port and providing for its security.

Promising Practices for Port Security

The study focused on local practices — that is, it excluded federal activities, such as those managed by the U.S. Department of Homeland Security or the U.S. Department of Justice.⁵ Although not included in the study, port security policies taken by the federal government before and after Sept. 11 were found to be key factors at all of the ports the researchers visited and to have had an impact on all ports in the United States. The study explored only cases where one of these nationwide practices had been adapted locally in a compelling manner.



The researchers identified practices in five general areas:

- Awareness of threats.
- Prevention of an attack.
- Preparedness for an attack.
- Response to an attack.
- Recovery after an attack.

They chose practices that stood out from the others because of their innovativeness, comprehensiveness or rigorous implementation.

Awareness of Threats

Awareness is heavily dependent on information sharing and requires a high level of cooperation among public and private sectors. The research revealed that the ports had undertaken two main efforts to increase awareness of an attack:

- Stakeholder coordination and collaboration initiatives.
- Protocols for detecting and monitoring port-related security risks.

The most notable promising practice in coordinating local stakeholders was the establishment of area maritime security committees (AMSCs). These committees (recommended in the 2002 Maritime Transportation Security Act) are made up of federal, state, local and private representatives who meet to identify and address vulnerabilities in and around ports and provide a forum for sharing information about port security issues. Although AMSCs existed at all the ports in the study, the groups varied considerably in size, stakeholders represented, frequency of convening and methods of functioning.

The research team also discovered a number of port-specific practices intended to detect and monitor security risks. These included port security teams within homeland security centers, recruiting a voluntary port security force to work in conjunction with the port police agency, and implementing Port Watch, similar to Neighborhood

Watch, which encourages tenants in the port to keep each other informed about security concerns.

Prevention of an Attack

Prevention practices are based on the premise that a strong, visible defense will deter an attack. The team identified a number of promising practices in preventing port attacks, including:

- Improvements to physical security and infrastructure at seaports.
- Protocols and processes limiting entry to seaports.
- Technological detection and inspection systems.
- Law enforcement-related activities.
- Interagency operational centers.

Measures included creating physical barriers, limiting access, installing detection equipment, increasing law enforcement activity and coordinating strategies among agencies. Seaports are difficult to defend because much of their perimeter is water. The researchers saw great potential in the development of the next generation of closed-circuit televisions (CCTVs) and sensors designed to detect chemical, biological, radiological and nuclear weapons of mass destruction, especially when they are used in combination with traditional security practices.

Some of the better systems combine CCTV and video analytics to analyze video proactively based upon observed behavior. Operators are trained to respond to certain anomalies or perceived threats. Another promising practice is the use of sensor technologies for screening, although there is still no technological substitute for good security procedures and well-trained human inspectors.

Not every prevention practice was high-tech or expensive. One simple strategy used by most of the ports visited was stacking empty shipping containers door-to-door. While not foolproof, stacking containers

with their doors facing each other is an easy way to block entry to terrorists, stowaways or smugglers who would seek to hide in shipping containers.

Preparedness for an Attack

Preparedness requires a measurable, demonstrated capacity to respond to threats with coordinated efforts by all essential participants, including elected officials; emergency services, fire, intelligence, medical, police and public health personnel; community organizations; the media; and the public at large.⁶ Port security officials with whom the researchers talked all agreed that they needed to increase their level of preparedness.

Terrorist attacks are rare, and few people have direct experience handling them. Therefore, the promising practices in this area are centered on various forms of training.

Awareness training for all port personnel is a low-cost approach that rapidly increases the number of people who are able to notice when something is amiss. Field exercises have also proven useful in simulating a potential attack and testing various aspects of the port's terrorism response plan. Ports are increasingly using models, games and simulations that prepare first responders for a seaport attack by letting them "experience" dangerous events without exposing them to hazards or accidental injury and without requiring the use of expensive resources such as personal protective equipment.

Response to an Attack

Responding to an attack against a port requires planning for uncertainty, fast action in moments of crisis and operations that almost always cross agency lines.⁷ The experts interviewed emphasized the need for federal, state, local and tribal authorities to rapidly assess the human and economic consequences and calculate the effects that could radiate to regional, national and global interests. Established contingency procedures can help ensure continuous operations and essential public services

and the resumption or redirection of maritime commercial activities to mitigate larger economic, social and national security effects of an incident.

Many of the ports visited used the Incident Command System (ICS), which establishes a "unified command" whereby agency managers share decision-making responsibility. There is no formal leader; the agency overseeing emergency operations depends on the nature and location of the event. Individual agencies maintain operational control of their own personnel and assets, and agency leaders act cooperatively, transferring decision-making authority within the unified command group based on the nature of an incident. This system allows agencies to adapt to changing situations as an incident unfolds by avoiding a rigid organizational structure. However, the effectiveness of this promising practice hinges on trust, cooperation and a clear understanding of which agency leads under what circumstances.⁸

Another promising practice is a team response model, which fosters strong partnerships among various first responders, such as firefighters, hazardous waste experts and medical personnel.

Recovery After an Attack

Recovery is a vitally important issue, because billions of dollars worth of cargo pass through the U.S. port system on a daily basis. Delays in reopening port facilities could result in dramatic, long-term economic (and other) consequences on a national and international scale.⁹

Compared to the other four areas, the research team did not observe many promising practices in the area of recovery. This is unfortunate because effective recovery actions would go a long way toward preserving life, property, the environment, and social, economic and political structures, as well as restoring order and essential services for those who live and work in the maritime domain.

One promising practice observed at two ports was the adoption of a consequence-management approach, which addresses

ways to alleviate the short- and long-term physical, socioeconomic and psychological effects of a catastrophe.¹⁰ Consequence-management exercises demand that seaport personnel and stakeholders consider essential issues in advance, such as when the port would reopen, which cargo would get priority, how passengers should be handled and what are the long- and short-term economic impacts of a complete shutdown.

Moving in the Right Direction

Researchers identified a number of promising practices but could not determine which were the best because data to conduct an evaluation do not exist. Although federal legislation requires certain minimum security practices, each port must consider and assess the relevance and effectiveness of the identified promising practices on an individual basis.

In the end, there were no magic solutions to assist the port community with the monumental task of protecting the nation's ports against a terrorist attack. But it is clear that seaports are aware of the dangers and are making strides toward securing the maritime domain. Sharing promising practices with each other — through discussions generated by research, U.S. Coast Guard conferences and local maritime security meetings — may well be one of the most promising actions we can take in safeguarding our country's seaports.

NCJ 225763

About the Authors

Bruce Taylor is the director of research at the Police Executive Research Forum (PERF) in Washington, D.C. He has more than 15 years of experience in research and survey design, randomized field experiments, and program evaluation. Before joining PERF, he was a managing associate at Caliber Associates, the deputy director of the Arrestee Drug Abuse Monitoring (ADAM) program at the National Institute of Justice, and a senior associate with the New York City Victim Services Agency.

Pat Kaufman is an attorney and freelance writer with more than 10 years of experience in legal writing and editing, mainly in the areas of drug enforcement, particularly in Fourth Amendment privacy and search and seizure issues; criminal drug testing involving violations of probation and supervised release by drug offenders; and corrections law.

For More Information

- Pate, A., B. Taylor, and B. Kubu, *Protecting America's Ports: Promising Practices*, final report submitted to the National Institute of Justice, U.S. Department of Justice, Washington, DC: January 2008 (NCJ 221075), available at www.ncjrs.gov/pdffiles1/nij/grants/221075.pdf.

Notes

1. A year after the Sept. 11 attacks, the U.S. Congress enacted the Maritime Transportation Security Act of 2002 (MTSA), a sweeping law that provided an overall planning and response framework for securing the nation's ports. Tasked with implementing many of the MTSA measures, the Coast Guard became the lead agency in maritime and port security. The United States also worked with the United Nations International Maritime Organization to promulgate new international requirements to strengthen maritime security.
2. Council on Foreign Relations, *Terrorism: Questions and Answers*, Washington, DC: Council on Foreign Relations, 2002.
3. Ervin, C.K., *Open Target: Where America Is Vulnerable to Attack*, New York: Palgrave Macmillan, 2006: 118.
4. Although we have chosen in this article not to cite specific ports by name when discussing promising practices, detailed information on the practices of each of the 17 ports is available in our full report.
5. Although the federal measures were not included in our study, we offer a full review of all these efforts in our final report.
6. RAND Corporation, *The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, Arlington, VA: RAND, December 15, 2003, available at www.globalsecurity.org/security/library/report/2003/volume_v_report_only.pdf.
7. Haveman, J., and H.J. Shatz, "Introduction and Summary," in *Protecting the Nation's Seaports: Balancing Security and Costs*, ed. J. Haveman and H.J. Shatz, San Francisco: Public Policy Institute of California, 2006: 1–30.
8. Ibid.
9. Ibid.
10. Seiple, C., "Domestic Response to Weapons of Mass Destruction," *Parameters* (Autumn 1997): 119–134.