

Securing the Nation's Seaports: Multiple Goals, Uncertain Results

The recent controversy over foreign management of cargo terminals at six U.S. seaports highlighted just how sensitive and problematic the issue of U.S. port security remains, more than four years after the September 11 terrorist attacks. The nation's 361 ports are seen by most security experts as attractive targets for a terrorist attack because they are so vital to the country's economy: About \$807 billion worth of goods passed through American seaports in 2003, 41 percent of all U.S. international trade. Moreover, millions of American paychecks depend on the efficient and secure flow of manufactured goods into U.S. ports from an increasingly global economy. Even before September 11, federal legislators and executives had begun contemplating myriad new programs, many of which they quickly implemented afterwards. But the process remains largely still under construction.

A new report from the Public Policy Institute of California, *Protecting the Nation's Seaports: Balancing Security and Cost*, examines in detail the full dimensions of the task of port security, the effectiveness of measures undertaken so far, and the costs to the nation—both of implementing adequate port security and of failing to do so. Economists Jon D. Haveman and Howard J. Shatz of PPIC teamed with an array of additional experts to marshal a broad overview of port security issues, to examine progress made since September 11, and to suggest how that progress might best be continued. The resulting compilation is a comprehensive assessment. It includes projections of the effects on the national economy of a successful port attack, the private-sector implications of improving port security, a first-hand account of the considerable bureaucratic challenges that still must be overcome at the level of individual ports, and guidelines for financing port security efforts.

Among the highlights:

- Shipping containers are a key vulnerability in the global maritime supply chain system. Containers, the vast majority of which remain uninspected, can serve terrorists in several different ways, and myriad loopholes in global regulations make the container system easily exploitable.
- The creation of comprehensive port attack recovery plans could do much to mitigate the effects of a port terrorist attack, through the reduction of post-attack economic panic and the quick restoration of global supply chains.
- Federal officials should reconsider the adequacy of current port security funding and staffing levels. These have not kept pace with the plethora of new, but often conflicting, programs and initiatives created in the wake of the September 11 attacks.

According to the report's authors, "Better policy guidance is needed. The U.S. government has demanded the implementation of multiple programs simultaneously, without setting priorities."

From a politician's point of view, port security emergency response planning is the worst of all worlds: it requires extremely high up-front costs for benefits that will be realized only in the future—most likely when the official is already out of office, and maybe never.

— from Chapter 6

Possible Economic Consequences of a Port Attack

Predictions about the financial costs to the nation of terrorist attacks on the United States can and do vary wildly in the popular imagination. In this report, two teams of researchers bring some realism to this question. Through different methods, the two teams create a range of possible economic consequences of a hypothetical attack on a major American port, such as Los Angeles–Long Beach. Combined, that port complex processed about \$243 billion worth of goods in 2004, or about 10 percent of all U.S. trade; its disruption could have national economic effects.

Edward E. Leamer and Christopher Thornberg of the UCLA Anderson Forecast contend in their analysis that these effects would not be nearly as dire as common wisdom might

assume. Using historical data, they compare a port closure caused by a terrorist attack to similar port closures throughout the country's history caused by labor disputes. During such closures, they argue, the economy was able to bounce back relatively quickly from the reduction in the flow of goods through the ports, even from unexpected shutdowns caused by wildcat strikes. Leamer and Thornberg note further that even the attacks of September 11, although creating a deep national psychological shock and hurting certain industrial sectors, did not result in long-lasting economic damage.

Authors Peter Gordon, James Moore, II, and Harry W. Richardson of the University of Southern California and Qisheng Pan of Texas Southern University argue that the effects of an attack on the Los Angeles–Long Beach port complex, especially one involving radiological weapons, could be very costly. The authors hypothesize a simultaneous attack that isolates Terminal Island, through which more than half of all Los Angeles–Long Beach trade flows. They estimate that a shutdown lasting a year could cause as much as \$45 billion in national economic damage, including direct costs, indirect costs, and induced costs—those resulting from reductions in spending by families of employees in affected industries.

Practices and Vulnerabilities

Containers, which revolutionized global maritime trade, draw the attention of two security experts from the University of California at Berkeley. In his chapter, Stephen S. Cohen analyzes the circuitous global journeys of the containers, more than 10 million of which arrive here every year. The threats they pose to security are numerous, Cohen finds, because of the physical impossibility of inspecting all of them, their critical position within just-in-time production systems, and difficulties in tracking them outside U.S. borders. Cohen suggests that a layered defense using multiple technologies, including radiation detectors, may provide the optimal, if expensive, defense.

Jay Stowsky examines the technologies of maritime security and container security in detail—specifically, how government can best encourage the private sector to further develop tools for container surveillance, tracking, and screening. Maritime dual-use technology development should follow a more flexible model than past dual-use practices, Stowsky argues, when large, government-funded systems had limited

outside applicability. In the current environment, where wide adoption of common security technologies by players in a globally dispersed sector is the objective, the government would do better to encourage independent research and development and faster, more efficient procurement practices.

Providing security in a large and complex port operation such as Los Angeles–Long Beach, the fifth-busiest container operation in the world, is made especially difficult by the multiple layers of bureaucracies with responsibility for some aspect of port operations and security, according to another of the report's research teams. Amy B. Zegart of the University of California at Los Angeles and Matthew C. Hipp and Seth K. Jacobson of the Riordan Institute for Urban Homeland Security personally worked over a period of years with the 15 agencies from five political jurisdictions that have port responsibility, to improve emergency response to a port incident. Their chapter details just how and why that was and remains such an arduous undertaking. In addition, politics can severely hinder port security efforts, the team found.

Programs and Costs

Editors Haveman and Shatz provide two in-depth analyses of the current state of maritime security, one detailing the responsibility and operations of the multiplicity of current federal programs now in place and the second analyzing how the nation attempts to pay for all of them. Four major programs covering responsibilities including ship and port security plans, container security, overseas ports, and grants for individual jurisdictions now regulate one or more aspects of the problem. Among the initial shortcomings of these, the authors find, were the failure to include labor groups in port security planning, competing legislation covering the same tasks, reliance on voluntary actions with limited verification and monitoring, and inadequate funding. In their analysis of costs, the authors find that the private and public sectors each have an important role in bearing the total cost of port security, which will likely be in the tens of billions of dollars. However, the proper balance between private and public costs remains an unresolved issue. Among the payment sources that have been suggested are user fees, diversion of customs revenues, and general government revenues. The best source of public funds is general government revenue, the authors conclude, with regulatory requirements that the private sector would have to meet and pay for through methods they devise.

*This research brief summarizes a report edited by Jon Haveman and Howard Shatz, *Protecting the Nation's Seaports: Balancing Security and Cost* (2006, 296 pp. \$25.00, ISBN 1-58213-120-1). The report may be ordered online at www.ppic.org or by phone at (800) 232-5343 or (415) 291-4400 [outside mainland U.S.]. A copy of the full text is also available at www.ppic.org. The Public Policy Institute of California is a private, nonprofit organization dedicated to independent, objective, nonpartisan research on economic, social, and political issues affecting California.*
