Executive Memorandum

Published by The Heritage Foundation

No. 980
September 22, 2005

Taking a Global Approach to Maritime Trade Security

Alane Kochems

All too often, security analysts have warned of a doomsday scenario in which terrorists use a cargo container to smuggle a nuclear bomb into the United States and detonate it in a major port, causing death and destruction, paralyzing shipping and ports around the world, and causing billions of dollars in damages. This is, in fact, one of the least likely forms of terrorist attack, yet this scenario is being used to argue for wrongheaded security solutions that would yield minimal benefits while costing billions of dollars and hamstringing global commerce.

- The United States should not attempt to make each cargo container and port into a miniature Fort Knox.
- The U.S. should improve supply chain security by strengthening existing components through better integration of commercial information and intelligence.

As a matter of common sense, the United States should not attempt to make every cargo container and port into a miniature Fort Knox. Securing trade requires a more comprehensive and effective approach than just putting up fences and gates, posting guards at ports, and inspecting all cargo containers as they enter the country. Efforts to protect trade should focus on improving security of the entire supply chain, not on creating isolated, easily bypassed chokepoints to address specific (and unlikely) threats. Strengthening existing programs could improve security *and* facilitate global commerce.

Global Trade and Global Terrorism. Maritime trade has become an increasingly important part of the global economy. It consists primarily of large containers shipped through megaports as part of a system of just-in-time deliveries and rolling inventories. In addition to using cargo containers to smuggle materials, weapons, and humans, global terrorists can use maritime commerce to raise money and to move and validate fraudulent documents. In this respect, global sea trade is no different from any other form of worldwide commerce or travel. Terrorists will try to exploit every aspect of maritime commerce.

However, some security analysts argue that container security should receive special consideration because a container could possibly be used to smuggle a nuclear weapon into the country. To counter this threat, they propose spending billions of dollars on container and port security.

This argument fails on four counts. First, the nuke-in-box is an unlikely terrorist tactic. If an enemy wanted to smuggle a bomb into the United States, a private watercraft would be a safer and more secure way to transport the weapon, either directly to the target (e.g., a port) or indirectly by

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/em980.cfm

Produced by the Kathryn and Shelby Cullom Davis
Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

landing it in Mexico and then driving it across the border. Second, while nuclear smuggling is possible, so are dozens of other attack scenarios. It is dangerously myopic to overinvest in countering one tactic when the terrorists could easily employ another tactic. Third, searching every container and hardening every port is an extremely inefficient and expensive way to stop terrorists from using cargo containers. Fourth, there is no viable business case for many of the proposed solutions for "hardening" shipping containers. These measures would provide only minimal utility at the cost of billions of dollars in new duties or taxes.

A Global Approach. Cargo containers are just one of many aspects of commercial shipping that should be considered in developing a comprehensive trade security strategy. The United States should approach cargo and port security from the perspective of the global supply chain rather than attempting (and failing) to make ports and containers impervious. Just as the terrorist threat is global, the security response needs to be global. As with much of homeland security, trade security is a matter of prioritizing and balancing risks.

The United States and the international community have already taken some steps to improve global trade security. For example, the Customs and Border Protection (CBP) Container Security Initiative (CSI) currently screens about 70 percent of all maritime containers shipped to the United States. The program works with 38 ports throughout the world, including the 20 ports that export the most (by volume) to the U.S. CBP also uses the Automated Targeting System (ATS) to identify high-risk containers. As part of the identification process, ships are required to provide manifests 24 hours before departure. High-risk containers are inspected using advanced radiation detection and large-scale imaging technology before they even reach U.S. shores. One criticism of ATS is that it does not draw from a broad enough array of commercial data sources to identify high-risk containers.

The Customs–Trade Partnership Against Terrorism (C–TPAT), another CBP program, allows companies that have taken voluntary steps to secure their containers and supply chains to move more quickly through the inspection process and undergo fewer inspections. This program gives companies incentives to tighten their supply-chain practices, improving overall security. It creates a win-win situation for both U.S. trade security and the companies that comply.

At the international level, the International Maritime Organization (IMO) has established the International Ship and Port Facility Security (ISPS) Code, which is a multilateral ship and port security standard. It requires all countries to submit port facility and ship security plans to the organization, thus making port security a shared responsibility among states and shipping authorities. Regrettably, many countries are still not in compliance with the code.

Undoubtedly, these programs can and should be improved. One U.S. priority should be to screen incoming cargo more intelligently by combining commercial data with intelligence information and analysis of trade patterns and the parties involved. Commercial data should include information such as a ship's past ports of call, scheduled destinations, and cargoes. These tactics need to be coupled with tighter supply-chain practices, better ship and employee scans, and more international cooperation on security.

A Better Way. While terrorists could use a cargo container to launch an attack on the United States, it is neither the most likely nor the most probable means of attack. Instead of focusing on preventing a low-probability attack, the United States could better secure itself by taking a global approach to trade security. The ISPS Code, C–TPAT, and CSI are all good and cost-effective components of a larger trade security strategy.

Now the U.S. needs a comprehensive approach to supply-chain security that includes these components and strengthens them by better integrating commercial information and intelligence. As part of the homeland security reorganization, Secretary of Homeland Security Michael Chertoff should ensure that the department's Chief Intelligence Officer makes this task a top priority.

—Alane Kochems is a Policy Analyst for National Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.