This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL
REPORT

Evaluating the Security of the Global Containerized Supply Chain

Henry H. Willis, David S. Ortiz

INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

The research described in this report results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by donors and by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers.

Library of Congress Cataloging-in-Publication Data

Willis, Henry H.
Evaluating the security of the global containerized supply chain / Henry H. Willis, David S. Ortiz.
p. cm.
"TR-214."
Includes bibliographical references.
ISBN 0-8330-3715-3 (pbk. : alk. paper)
1. Shipping—Security measures. 2. Unitized cargo systems—Safety measures. 3. Container ports—Security measures—United States. 4. Marine terminals—Security measures—United States. 5. Terrorism—United States—Prevention. I. Ortiz, David (David Santana) II.Title.

HE735.W55 2004
363.32—dc22

2004024937

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

Published 2004 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

The global supply chain is the network of suppliers, manufacturing centers, warehouses, distribution centers, and retail outlets that transforms raw materials into finished products and delivers them to consumers (Simchi-Levi, Kaminsky, and Simchi-Levi, 2002). Security of the system has traditionally focused on reducing shrinkage—the loss of cargo shipments through theft and misrouting. However, heightened awareness of terrorism has redefined supply-chain security—the consequences of an attack on or via a critical global port could be a tremendous loss of life and a crippling of the U.S. economy—and has brought increased attention to the risks containerized shipping presents.

The response has been proliferation of new security measures. For all these efforts, is the system of trade more or less secure? Will we know if these efforts are successful? How will success or failure be measured? This report presents a strategy for answering these questions using methods for managing risk of large-scale systems to analyze the structure of the container supply chain and its properties.

The Three Layers of the Global Container Supply Chain

The structure of the global container supply chain would seem self-evident: It is a system of vessels, port facilities, railcars, trucks, and containers that transport goods in discrete units around the earth. That view, however, pertains only to the physical components of a system that includes the cargo, information, and financial flows required for the system to operate. We propose viewing the supply chain as three interdependent and interacting networks: a physical logistics system for transporting goods; a transaction-based system that procures and distributes goods and that is driven primarily by information flows; and an oversight system that implements and enforces rules of behavior within and among the subsystems through standards, fines, and duties. Network components are *nodes*, such as factories and ports, and *edges*, such as roads and information links. Figure S.1 illustrates the subsystems as a collection of layers. The oversight system has agencies and organizations that interact with the layers of the global container supply chain. The different points of view of the supply chain can be viewed in terms of a layered set of networks. The *logistics layer* is responsible for the movement of cargo along a network of roads; the *transaction layer* orders goods and materials from a network of suppliers; and the *regulatory layer* specifies standards for operation within its area of authority.

Table S.1 lists examples of the organizations present in each layer. The three layers may be specified by the organizations that comprise each. Note that oversight agencies have a limited range of influence over organizations in either the transaction or logistics layer.

Figure S.1
Interactions Between the Logistics, Transaction, and Oversight Layers of the Supply Chain. The different points of view of the supply chain can be viewed in terms of a layered set of networks. The logistics layer is responsible for the movement of cargo along a network of roads; the transaction layer orders goods and materials from a network of suppliers; and the regulatory layer specifies standards for operation within its area of authority.

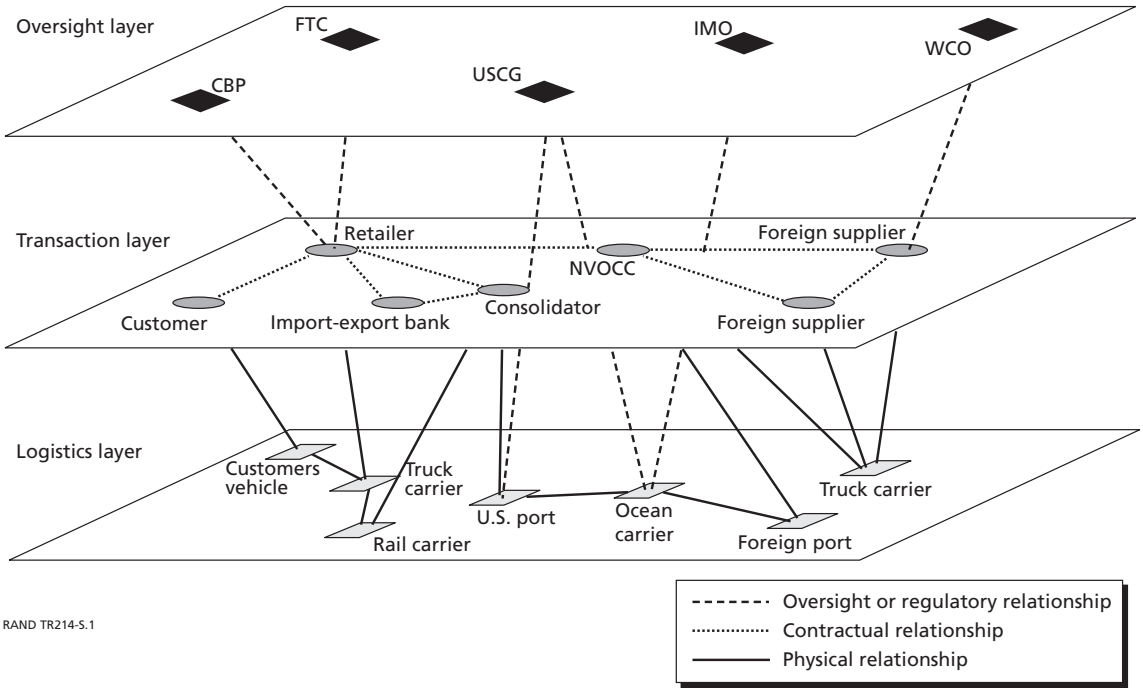

Table S.1
Organizational Interests. The three layers may be specified by the organizations that comprise each layer. Note that oversight agencies have a limited range of influence over organizations in either the transaction or logistics layer.

Layer	Examples of Stakeholders	Examples of Oversight Agencies
Transaction	Wal-Mart Target Ford Non–Vessel-Operating Common Carriers (NVOCCs)	Federal Trade Commission U.S. Customs and Border Protection World Customs Organization
Logistics layer	International Longshore and Warehouse Union Pacific Maritime Association International Labor Organization CSX Transportation APL Maersk Sealand Port of Long Beach	U.S. Department of Labor U.S. Department of Homeland Security Local law enforcement U.S. Coast Guard U.S. Customs and Border Protection World Customs Organization

Examining the supply chain from each of these perspectives yields insights into the concerns of relevant stakeholders, the levers available to improve supply-chain performance, and the interactions among the layers that improve or detract from system performance.

Capabilities of the Global Container Supply Chain

The ability of the global container supply chain to deliver goods efficiently and securely can be described through five measurable capabilities:

- **Efficiency**. Container shipping has evolved primarily to deliver goods more quickly and more cheaply than other modes of transport, when volume and mass are taken into account.
- **Shipment reliability.** Supply chains must behave as expected, retrieving and delivering goods as directed, with a minimum amount of loss due to theft and accident.
- **Shipment transparency.** The goods that flow through a supply chain must be legitimately represented to authorities and must be legal to transport.
- **Fault tolerance.** The container shipping system should be able to respond to disruptions and failures of isolated components without bringing the entire system to a grinding halt.
- **Resilience.** A supply chain is resilient insofar as it is able to return to normal operating conditions quickly after the failure of one or more components. Resilience is a function of both the system's design and the responsiveness of the oversight layer.

The efficiency of the container shipping system is measured in terms of its speed and cost, taking reliability into account. Security, however, is a function of the final four capabilities. Efficiency and security are often portrayed as in direct conflict, but in our formulation, they are measured differently and may support or hinder one another, depending on the circumstances. Analysis of any program's efficiency and security implications needs to consider the system under both normal and emergency operating conditions.

Managing Risk in the Global Container Supply Chain

We applied a framework of technology-induced risk assessment (Morgan, 1981) to provide insight into how supply-chain security capabilities are realized. Table S.2 details how policy and technology proposals support improved supply-chain capabilities. This table presents the perspective of capabilities that could be captured by private shippers, carriers, and port operators and by the U.S. government. Through application of this methodology, we also get a high-level view of how these objectives come together as an integrated container security strategy. The methodology also reveals gaps in the set of policies intended to improve the security of the global container supply chain: fault tolerance and resilience, for instance, have received little attention from policymakers.

Table S.2
Examples of How Preparedness Strategies May Influence the Exposure-Effects Chain of Notional Terrorist Events

			Anticipated Supply Chain Security Effects			
			Threat or Vulnerability Reduction		Consequence Reduction	
Policy or Technology	Driving Layer	Anticipated Supply Chain Efficiency Effects	Reduce Probability of Attack	Reduce Probability of Successful Attack	Avoid or Modify Attack Consequences	Mitigate or Compensate for Consequences
Customs-trade partnership against terrorism	Transaction and logistics	Reduced shipping cost and time and increased volume: *Expedited customs*	Reduced damage, losses, and fraud: *Deter terrorists, thieves, and smugglers*			
Operation Safe Commerce	Logistics and oversight			Reduced fraud: *Detect at entry*		
Container security initiative	Oversight			Reduced damage and fraud: *Detect at origin*		
Maritime Transportation Security Act of 2002	Oversight			Reduced theft: *Control access*		Increased Fault tolerance and resilience: *Disaster planning*
Anti-tamper seals	Transaction and logistics			Reduced damage: *Detect at origin* Reduced fraud: *Detect at origin or entry*		
Radio frequency identification	Transaction and logistics	Reduced shipping cost and time: *Improved Logistics*		Reduced theft losses: *Detect unapproved transport* Reduced damage: *Detect at origin* Reduced fraud: *Detect at entry or origin*		Increased resilience: *Rapid location and rerouting of shipments following a disaster*
X-ray and gamma-ray inspection	Logistics and oversight			Reduced damage: *Detect at origin* Reduced fraud: *Detect at origin or entry*		
Radiation pagers, portal sensors, and remote monitoring	Logistics and oversight			Reduced damage: *Detect at origin*	Reduced damage: *Detection before cargo enters ports*	

Preliminary Conclusions

Applying the layered capabilities framework to the analysis of current efforts to improve supply-chain security led us to two conclusions:

- **Supply-chain efficiency and security are distinct but interconnected.** Efforts to improve the efficiency of the container shipping system may or may not have affected the security of the system. In turn, security efforts might also improve efficiency. Those that do not may lead to unexpected negative consequences as the system adapts to compensate for or work around resulting losses of efficiency.
- **Both public- and private-sector initiatives to improve the security of the global supply chain have focused largely on preventing and deterring smuggling and terrorist attacks.** These initiatives focus on improving the transparency of the global container supply chain. Few initiatives have focused on improving the fault tolerance or resilience of the system, which could be a fruitful area for new security measures.

Recommendations

These conclusions suggest three complementary paths for improving the security of the global container supply chain while maintaining its efficiency:

- **The public sector should seek to bolster the fault tolerance and resilience of the global container supply chain.** The closure of a major port—for whatever reason—would have a significant effect on the U.S. economy. The federal government should lead the coordination and planning for such events for two reasons. First, the motivation of the private sector to allocate resources to such efforts is subject to the market failures of providing public goods. Second, the government will be responsible for assessing security and for decisions to close and reopen ports.
- **Security efforts should address vulnerabilities along supply-chain network edges.** Efforts to improve the security of the container shipping system continue to be focused on ports and facilities (although many ports around the world still failed to meet International Ship and Port Security Code guidelines even after the July 1, 2004, deadline.) Unfortunately, the route over which cargo travels is vast and difficult to secure. Measures to keep cargo secure while it is en route are essential to a comprehensive strategy to secure the global container supply chain.
- **Research and development should target new technologies for low-cost, high-volume remote sensing and scanning.** Current sensor technologies to detect weapons or illegal shipments are expensive and typically impose significant delays on the logistics system. New detection technologies for remote scanning of explosives and radiation would provide valuable capabilities to improve the security of the container shipping system.

Future Inquiry

This report is our initial assessment of the security of the global container supply chain; our work is continuing in the following areas:

1. assessment of policies for improving supply-chain security
2. systems analysis of supply-chain risk
3. technology assessment and research and development planning for improving supply-chain performance
4. economic analysis of global trade trends on supply-chain performance.