

April 15, 2006

## The Global Supply Chain

### Maritime trade poses urgent security challenge

*The recent purchase by Dubai Ports World of a British shipping company would have given the United Arab Emirates-owned company control over the terminal operations in six major U.S. Ports (New York, Miami, Newark-Port Elizabeth, Philadelphia, New Orleans and Baltimore).*

*News of the deal created an outcry and opposition in Congress and among the public, which eventually led to the company agreeing to give up its stake in U.S. Ports. This incident has stirred a renewed interest in port and maritime security and drawn attention to its troubling weaknesses.*

*This issue of The Lipman Report examines the current state of maritime security and what needs to be done to make the global supply chain more secure.*

#### Maritime trade

Maritime trade is vital to the United States economy. Approximately 95 percent by volume of the nation's overseas cargo moves through ports and \$1.3 billion worth of goods moves in and out of U.S. ports every day. In addition, more than half of America's population lives within 50 miles of the coasts, and many major urban areas and critical infrastructure are near to or accessible by U.S. ports and waterways.

Over the next two decades maritime commerce likely will become an even larger and more important part of the global economy. To improve efficiency and lower their costs, maritime shippers increasingly concentrate their traffic through a smaller number of major cargo hubs. In the United States, 50 ports account for approximately 90 percent of all cargo tonnage. Their specialized equipment is essential for the loading and unloading of container ships, which constitute a growing segment of maritime commerce.

In 2005, U.S. seaports unloaded approximately 11 million containers, which was nearly 25 percent more than in 2000. Industry experts forecast that this volume will more than double within 20 years. The explosive growth in containerized shipping has dramatically lowered the costs and improved the reliability of the global supply chains that virtually all companies rely upon.

The economic, physical and psychological damage that would result from a significant terrorist attack targeting maritime commerce or taking advantage of the United States' potential vulnerability to sea attacks is difficult to estimate but the consequences would likely be enormous. A significant interruption of the maritime transport system would send shockwaves through the world economy. A large attack could potentially stop the global trade system as nations struggle to recover. In the wake of such an attack, governments are likely to adopt drastic and inefficient security measures that would significantly disrupt port operations due to cargo checks at both originating and destination ports.

#### One scenario for a terrorist attack

A container of athletic foot wear for a name brand company is loaded at a manufacturing plant overseas. The container doors are shut and a mechanical seal is put on it. These designer sneakers are destined for retail stores in malls across America. The container and seal numbers are recorded at the factory. A local truck driver, sympathetic to al Qaeda picks up the container.

On the way to the port, he turns into an alleyway and backs up the truck at a nondescript warehouse where a small team of operatives pry loose one of the door hinges to open the container so that they can gain access to the shipment. Some of the sneakers are removed and in their place, the operatives load a "dirty bomb" wrapped in lead shielding, and they then refasten the door.

The driver takes the container, now loaded with a "dirty bomb," to the local port where it is loaded on a coastal feeder ship carrying about 300 containers for its voyage. Later, the container is transferred to another ship which typically carries 1200-1500 containers to another port. In this case, the container is loaded on a super-container ship that carries 5000-8000 containers for a trans-Pacific voyage.

The container is then off-loaded in North America. Because it originates from a trusted-name brand company that has joined the volun-

**(continued on next page)**

## The Global Supply Chain

### Maritime trade poses urgent security challenge

(continued from preceding page)

tary government-business initiative to strengthen the global supply chain, Customs-Trade Partnership Against Terrorism (C-TPAT), the shipment is never identified for inspection by the Container Security Initiative team.

Consequently, the container is loaded directly from the ship to a railcar where it is shipped to a rail yard in an American city. Because the “dirty bomb” is shielded in lead, radiation portals do not detect it. When the container reaches a distribution center, a triggering device attached to the door sets the bomb off.

#### Devastating consequences

There would be four immediate consequences associated with such an attack. First, there would be the local deaths and injuries associated with the blast of the conventional explosives. Second, there would be the environmental damage done by the spread of industrial-grade radioactive material. Third, there would be no way to determine where the compromise to security took place so the entire supply chain and all the transportation nodes and providers must be presumed to present a risk of a potential follow-on attack. Fourth—and perhaps most importantly—all the current container and port security initiatives would be compromised by the incident.

#### Nature of the threat

The previous scenario illustrates the complex nature of the maritime security challenge. First, the threat is not so much tied to seaports and U.S. borders as it is to global supply chains that now largely operate on an honor system because standards are so nominal. Second, no transportation provider, port operator, or border inspector really knows what is in the containers that pass through their facilities and the radiation portal technology currently being deployed at U.S. borders can be evaded by placing light shielding around a weapon. Third, private companies must be a part of the solution since they have huge investments at stake. Fourth, the challenge of securing global supply chains can involve both port security

and border security measures simultaneously when containers are shipped overseas and then cross national borders.

The opportunities for terrorists to target legitimate global supply chains remain plentiful and the motivation for doing so is only growing as terrorists gravitate towards economic disruption as a major tactic in their war with the United States and the West. Against this strategic backdrop, there remains too little appreciation within the U.S. government that global supply chains and the transportation system that supports them remain very vulnerable to mass disruption. Instead, U.S. border agencies and the national security community have been looking at supply chains as one of a variety of smuggling venues. For the foreseeable future, the material to make a dirty bomb will likely be available throughout the international community despite stepped-up counter-proliferation and the threat to the global supply chain will remain urgent.

#### Current state of the global supply chain

The vast number of U.S. government initiatives since 9/11 suggests that substantial progress is being made in securing the global trade and transportation system. Unfortunately, the approach to date has been a piecemeal one, with each agency pursuing its signature program or programs with little regard for the other initiatives. There are also vast disparities in the resources that the agencies have been allocated. But more problematic are some of the questionable assumptions about the nature of the terrorist threat that underpin these programs.

New “risk management” programs advanced by the Customs and Border Protection Agency (CBP) are especially vulnerable to being discredited should terrorists succeed at detonating a “dirty bomb” smuggled into the country in a shipping container. Customs inspectors rely primarily on their past experience in identifying criminal or regulatory misconduct to determine if a containerized shipment might potentially be compromised. The GAO has documented glaring weaknesses with the methodology, underlying assumptions, and execu-

tion of Customs' practices in targeting containers.

Prior to 9/11, the cornerstone of the risk assessment framework used by customs inspectors was to identify "known shippers" that had an established track record of being engaged in legitimate commercial activity and playing by the rules. Since 9/11, the agency has built on that model by extracting a commitment from shippers to follow the supply chain security practices outlined in the Customs-Trade Partnership Against Terrorism. As long as there is not specific intelligence to tell inspectors otherwise, shipments from C-TPAT companies are viewed as presenting little risk.

The problem with this approach is that what may have made sense for combating crime does not automatically translate to combating determined terrorists.

Terrorists are likely to find it particularly attractive to target a legitimate company with a well-known name precisely because they can count on these shipments entering the United States with a only a cursory look or no inspection at all. It is well known which companies are viewed by U.S. customs inspectors as "trusted" shippers.

Many companies who have enlisted in C-TPAT have advertised their participation. In public speeches, senior U.S. Customs officials have singled out several large companies by name as model participants in the program. So all a terrorist need do is to find a single weak link within a "trusted" shipper's complex supply chain, such as a poorly paid truck driver taking a container from a remote factory to a loading port.

In all likelihood, when the next terrorist attack occurs on U.S. soil and it involves a maritime container it will have come in contact with most or even all the security protocols. As a consequence, when the attack happens, the entire security regime will be implicated generating tremendous political pressure to abandon it.

### **Security improvements**

With relatively modest investments and a bit of

ingenuity, the international system and global supply chains can have credible security while simultaneously improving their efficiency and reliability.

What is required are a series of measures that collectively enhance visibility and accountability within global supply chains. As a starting point, the United States should work with the Association of Southeast Asian Nations (ASEAN) and the European Union (EU) in authorizing third parties to conduct validation audits of the security protocols contained in the International Ship and Port Facility Security Code and the World Customs Organization's new framework for security and trade facilitation.

To minimize the risk that containers will be targeted by terrorist organizations between the factory and a loading port, the next step must be for governments to create incentives for the speedy adoption of technical standards developed by the International Standards Organization for tracking a container and monitoring its integrity. The Radio Frequency Identification (RFID) technologies now being used by the U.S. Department of Defense for the global movement of military goods can provide a model for such a regime.

Washington should next embrace and actively promote the widespread adoption of a novel container security project being sponsored by the Container Terminal Operators Association (CTOA) of Hong Kong.

Starting in late 2004, every container arriving in the two main truck gates of two of the busiest marine terminals in the world have been passing through a gamma ray machine to scan its contents, a radiation portal to record the levels of radioactivity found within the container, and optical character recognition cameras which photograph the number painted on the top, back, and two sides of the container. These scanned images, radiation profiles, and digital photos are then stored in a database for customs authorities to access if and when they want.

**(continued on next page)**

## The Global Supply Chain

### Maritime trade poses urgent security challenge

(continued from preceding page)

This low-cost system of inspection is being carried out without impeding the operations of these very busy marine terminals. It could be put in place in every major container port in the world at an estimated cost of \$1.5 billion or approximately \$10-\$25 per container, depending on the volume of containers moving through the terminal. The system could be paid for by authorizing ports to collect user fees that cover the costs associated with purchasing the equipment, maintaining its upkeep, and investing in upgrades when appropriate. Once such a system is operating globally, each nation would be in a position to monitor its exports and to spot-check their imports against the images first collected at the loading port.

From the standpoint of U.S. security, the biggest value of this system should it be widely deployed are twofold. It provides a powerful deterrent to discourage terrorists from exploiting global supply chains as a conduit for a weapon of mass destruction and aids counterproliferation measures as well.

Also, it creates a powerful deterrent to discourage terrorists from targeting the global supply chains with a "dirty bomb" since the inspection system will make the system far more resilient in managing a breach of security without a wholesale shutdown of the trade system.

The total cost of third party compliance inspections, deploying "smart" containers, and operating a cargo scanning system such as the one being piloted in Hong Kong may reach \$50 to \$100 per container depending on the number of containers an importer has and the complexity of its supply chain. Such an investment would allow container security to quickly move to a much more secure system.

Even if there were no terrorist threat, there are ample reasons for individual governments, and other international organizations to place port, border, and transportation security at the top of the multilateral agenda. Enhancing controls within the global trade lanes will help all countries reduce theft; stop the smuggling of drugs,

humans, and counterfeit goods; crack down on tariff evasion; and improve export controls and security in general.

At the end of the day, confronting the nuclear smuggling threat requires that we take the post-9/11 security framework the U.S. government has been developing haphazardly over the past four years, and quickly move it to the next generation of initiatives that build on the original framework.

The three key elements for getting from where we are to where we must be are: (1) to recognize that it is a global network that we are trying to secure; (2) that much of that network is owned and operated by private entities, many who have foreign ownership so the U.S. government must be willing and able to work with those companies as well as their host governments so as to advance appropriate safeguards, and (3) both Congress and the White House should embrace a framework of "trust but verify," based on real global standards and meaningful international oversight.

*The size of the maritime domain makes the security challenge difficult and complex. In this security environment, responding to unpredictable and international threats requires cooperation and a continuing sense of vigilance. Shared steps for ensuring the security of containers at all points along the global supply chain should be developed, along with plans for maintaining continuity in the event of possible trade disruptions. The private and public sectors must adopt a more aggressive and innovative approach to maritime security, working together to create and enforce policies that enhance security.*



The Lipman Report Editors