FAR EASTERN ECONOMIC REVIEW

Essay

January/February 2006

Port Security Is Still A House of Cards

By Stephen E. Flynn

As one of the world's busiest ports, it is fitting that Hong Kong played host to the World Trade Organization's December 2005 meeting. After all, seaports serve as the on- and off-ramps for the vast majority of traded goods. Still, the leaders of the 145 delegations that convened in Hong Kong undoubtedly did not have much more than a sightseer's interest in the host city's magnificent and frenetic harbor. For the most part, finance and trade ministers see trade liberalization as involving efforts to negotiate rules that open markets and level the playing field. They take as a given the availability of transportation infrastructures that physically link markets separated by vast distances.

But the days when policy makers could take safe transportation for granted are long past. The Sept. 11, 2001 attacks on New York and subsequent attacks on Madrid and London show that transport systems have become favored targets for terrorist organizations. It is only a matter of time before terrorists breach the superficial security measures in place to protect the ports, ships and the millions of intermodal containers that link global producers to consumers.

Should that breach involve a weapon of mass destruction, the United States and other countries will likely raise the port security alert system to its highest level, while investigators sort out what happened and establish whether or not a follow-on attack is likely. In the interim, the flow of all inbound traffic will be slowed so that the entire intermodal container system will grind to a halt. In economic terms, the costs associated with managing the attack's aftermath will substantially dwarf the actual destruction from the terrorist event itself.

Fortunately, there are pragmatic measures that governments and the private sector can pursue right now that would substantially enhance the integrity and resilience of global trade lanes. Trade security can be improved with modest upfront investments that enhance supply chain visibility and accountability, allowing companies to better manage the choreography of global logistics—and, in the process, improve their financial returns. In short, there is both a public safety imperative and a powerful economic case for advancing trade security.

A Brittle System

Though advocates for more open global markets rarely acknowledge it, when it comes to converting free trade from theory to practice the now-ubiquitous cargo container deserves a great deal of credit. On any given day, millions of containers carrying up to 32 tons of goods each are moving on trucks, trains and ships. These movements have become remarkably affordable, efficient, and reliable, resulting in increasingly complex and economically expedient global supply chains for manufacturers and retailers.

From a commercial standpoint, this has been all for the good. But there is a problem: as enterprises' dependence on the intermodal transportation system rises, they become extremely vulnerable to the consequences of a disruption in the system. To appreciate why that is so requires a brief primer on how that system has evolved.

Arguably, one of the most unheralded revolutions of the 20th century was the widespread adoption of the cargo container to move manufactured and perishable goods around the planet. In the middle of the last century, shipping most goods was labor intensive: items had to be individually moved from a loading dock at a factory to the back of a truck and then offloaded and reloaded onto a ship. Upon arrival in a foreign port, cargo had to be removed by longshoremen from the ship's holds, then moved to dock warehouses where the shipments would be examined by customs inspectors. Then they were loaded onto another transportation conveyance to be delivered to their final destination. This constant packing and repacking was inefficient and costly. It also routinely involved damage and theft. As a practical matter, this clumsy process was a barrier to trade.

The cargo container changed all that. Now goods can be placed in a container at a factory and be moved from one mode of transportation to another without being manually handled by intermediaries along the way. Larger vessels can be built to carry several thousand containers in a single voyage. In short, as global trade liberalization accelerated, the transportation system was able to accommodate the growing number of buyers and sellers.

Arguably, East Asia has been the biggest beneficiary of this transportation revolution. Despite the distance between Asia and the U.S., a container can be shipped from Hong Kong, Shanghai, or Singapore to the West Coast for roughly $4,000. This cost represents a small fraction of the $66,000 average value of goods in each container that is destined for the U.S.

However, multiple port closures in the U.S. and elsewhere would quickly throw this system into chaos. U.S.-bound container ships would be stuck in docks, unable to unload their cargo. Marine terminals would have to close their gates to all incoming containers since they would have no place to store them. Perishable cargo would spoil. Soon, factories would be idle and retailers' shelves bare.

In short, a terrorist event involving the intermodal transportation system could lead to unprecedented disruption of the global trade system, and East Asia has the most to lose.

What Has Been Done?

The possibility that terrorists could compromise the maritime and intermodal transportation system has led several U.S. agencies to pursue initiatives to manage this risk. The U.S. Coast Guard chose to take a primarily multilateral approach by working through the London-based International Maritime Organization to establish new international standards for improving security practices on vessels and within ports, known as the International Ship and Port Facility Code (ISPS). As of July 1, 2004, each member state was obliged to certify that the ships that fly their flag or the facilities under their jurisdiction are code-compliant.

The Coast Guard also requires that ships destined for the U.S. provide a notice of their arrival a minimum of 96 hours in advance and include a description of their cargoes as well as a crew and passenger list. The agency then assesses the potential risk the vessel might pose. If the available intelligence indicates a pre-arrival security check may be warranted, it arranges to intercept the ship at sea or as it enters the harbor in order to conduct an inspection.

The new U.S. Customs and Border Protection Agency (CBP), which was established within the Department of Homeland Security, mandated that ocean carriers must electronically file cargo manifests outlining the contents of U.S.-bound containers 24 hours in advance of their being loaded overseas. These manifests are then analyzed against the intelligence databases at CBP's National Targeting Center to determine if the container may pose a risk.

If so, it will likely be inspected overseas before it is loaded on a U.S.-bound ship under a new protocol called the Container Security Initiative (CSI). As of November 2005, there were 41 CSI port agreements in place where the host country permits U.S. customs inspectors to operate within its jurisdiction and agrees to pre-loading inspections of any targeted containers.

Decisions about which containers will not be subjected to an inspection are informed by an importer's willingness to participate in another post-9/11 initiative, known as the Customs-Trade Partnership Against Terrorism (C-TPAT). C-TPAT importers and transportation companies agree voluntarily to conduct self-assessments of their company operations and supply chains, and then put in place security measures to address any security vulnerabilities they find. At the multilateral level, U.S. customs authorities have worked with the Brussels-based World Customs Organization on establishing a new framework to improve trade security for all countries.

In addition to these Coast Guard and Customs initiatives, the U.S. Department of Energy and Department of Defense have developed their own programs aimed at the potential threat of weapons of mass destruction. They have been focused primarily on developing the means to detect a "dirty bomb" or a nuclear weapon.

The Energy Department has been funding and deploying radiation sensors in many of the world's largest ports as a part of a program called the Megaport Initiative. These sensors are designed to detect radioactive material within containers. The Pentagon has undertaken a counterproliferation initiative that involves obtaining permission from seafaring countries to allow specially trained U.S Navy boarding teams to conduct inspections of a flag vessel on the seas when there is intelligence that points to the possibility that nuclear material or a weapon may be part of the ship's cargo.

Finally, in September 2005, the White House weighed in with its new National Maritime Security Strategy. This purports to "present a comprehensive national effort to promote global economic stability and protect legitimate activities while preventing hostile or illegal acts within the maritime domain."

A House of Cards

Ostensibly, the flurry of U.S. government initiatives since 9/11 suggests substantial progress is being made in securing the global trade and transportation system. Unfortunately, all this activity should not be confused with real capability. For one thing, the approach has been piecemeal, with each agency pursuing its signature program with little regard for other initiatives. There are also vast disparities in the resources that the agencies have been allocated, ranging from an $800 million budget for the Department of Energy's Megaport initiative to no additional funding for the Coast Guard to support its congressionally mandated compliance to the ISPS Code. Even more problematic are some of the questionable assumptions about the nature of the terrorist threat that underpin these programs.

In an effort to secure funding and public support, agency heads and the White House have oversold the contributions of these new initiatives. Against a backdrop of inflated and unrealistic expectations, the public is likely to be highly skeptical of official assurances in the aftermath of a

terrorist attack involving the intermodal transportation system. Scrambling for fresh alternatives to reassure anxious and angry citizens, the White House and Congress are likely to impose Draconian inspection protocols that dramatically raise costs and disrupt crossborder trade flows.

The new risk-management programs advanced by the CBP are especially vulnerable to being discredited, should terrorists succeed at turning a container into a poor man's missile. Before stepping down as commissioner in late November 2005, Robert Bonner repeatedly stated in public and before Congress that his inspectors were "inspecting 100% of the right 5% of containers." That implies the CBP's intelligence and analytical tools can be relied upon to pinpoint dangerous containers.

Former Commissioner Bonner is correct in identifying only a tiny percentage of containers as potential security risks. Unfortunately, CBP's risk-management framework is not up to the task of reliably identifying them, much less screening the low- or medium-risk cargoes that constitute the majority of containerized shipments and pass mostly uninspected into U.S. ports. There is very little counterterrorism intelligence available to support the agency's targeting system.

That leaves customs inspectors to rely primarily on their past experience in identifying criminal or regulatory misconduct to determine if a containerized shipment might potentially be compromised. This does not inspire confidence, given that the U.S. Congress's watchdog, the Government Accountability Office (GAO), and the U.S. Department of Homeland Security's own inspector general have documented glaring weaknesses with current customs targeting practices.

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 engaging in legitimate commercial activity. After 9/11, the agency expanded that model by extracting a commitment from shippers to follow the supply chain security practices outlined in C-TPAT. As long as there is no specific intelligence to tell inspectors otherwise, shipments from C-TPAT-compliant companies are viewed as low-risk.

The problem with this method is that it is designed to fight conventional crime; such an approach is not necessarily effective in combating determined terrorists. An attack involving a weapon of mass destruction differs in three important ways from organized criminal activity.

First, it is likely to be a one-time operation, and most private company security measures are not designed to prevent single-event infractions. Instead, corporate security officers try to detect infractions when they occur, conduct investigations *after* the fact, and adapt precautionary strategies accordingly.

Second, terrorists will likely target a legitimate company with a well-known brand name precisely because they can count on these shipments entering the U.S. with negligible or no inspection. It is no secret which companies are viewed by U.S. customs inspectors as "trusted" shippers; many companies enlisted in C-TPAT have advertised their participation. All a terrorist organization needs to do is 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 port. They can then gain access to the container in one of the half-dozen ways well known to experienced smugglers.

Third, this terrorist threat is unique in terms of the severity of the economic disruption. If a weapon of mass destruction arrives in the U.S., especially if it enters via a trusted shipper, the risk-management system that customs authorities rely on will come under intense scrutiny. In the

interim, it will become impossible to treat crossborder shipments by other trusted shippers as low-risk. When every container is assumed to be potentially high-risk, everything must be examined, freezing the worldwide intermodal transportation system. The credibility of the ISPS code as a risk-detection tool is not likely to survive the aftermath of such a maritime terrorist attack, and its collapse could exacerbate a climate of insecurity that could likely exist after a successful attack.

Moreover, the radiation-detection technology currently used in the world's ports by the Coast Guard and Customs and Border Protection Agency is not adequately capable of detecting a nuclear weapon or a lightly shielded dirty bomb. This is because nuclear weapons are extremely well-shielded and give off very little radioactivity. If terrorists obtained a dirty bomb and put it in a box lined with lead, it's unlikely radiation sensors would detect the bomb's low levels of radioactivity.

The flaws in detection technology require the Pentagon's counterproliferation teams to physically board container ships at sea to determine if they are carrying weapons of mass destruction. Even if there were enough trained boarding teams to perform these inspections on a regular basis—and there are not—there is still the practical problem of inspecting the contents of cargo containers at sea. Such inspections are almost impossible because containers are so closely packed on a container ship that they are often simply inaccessible. This factor, when added to the sheer number of containers on each ship—upwards of 3,000—guarantees that in the absence of very detailed intelligence, inspectors will be able to perform only the most superficial of examinations.

In the end, the U.S. government's container-security policy resembles a house of cards. In all likelihood, any terrorist attack on U.S. soil that involved a maritime container would come in contact with most, or even all, of the existing maritime security protocols. Consequently, a successful seaborne attack would implicate the entire security regime, generating tremendous political pressure to abandon it.

The Way Ahead

We can do better. The Association of Southeast Asian Nations should work with the U.S. and the European Union in authorizing third parties to conduct validation audits in accordance with the security protocols outlined in the International Ship and Port Facility Security Code and the World Customs Organization's new framework for security and trade facilitation.

A multilateral auditing organization made up of experienced inspectors should be created to periodically audit the third party auditors. This organization also should be charged with investigating major incidents and recommending appropriate changes to established security protocols.

To minimize the risk that containers will be targeted between the factory and loading port, governments should create incentives for the speedy adoption of technical standards developed by the International Standards Organization for tracking a container and monitoring its integrity. The technology now used by the U.S. Department of Defense for the global movement of military goods can provide a model for such a regime.

Asean and the EU should also endorse a pilot project being sponsored by the Container Terminal Operators Association (CTOA) of Hong Kong, in which every container that arrives passes through a gamma-ray content-scanning machine, as well as a radiation portal to record the levels of radioactivity within the container. Optical character recognition cameras then photograph the

number painted on several sides of the container. These scanned images, radiation profiles, and digital photos are then stored in a database where they can be immediately retrieved if necessary.

The marine terminals in Hong Kong have invested in this system because they hope that a 100% scanning regime will deter a terrorist organization from placing a weapon of mass destruction in a container passing through their port facilities. Since each container's contents are scanned, if a terrorist tries to shield radioactive material to defeat the radiation portals, it will be relatively easy to detect the shielding material because of its density.

Another reason for making this investment is to minimize the disruption associated with targeting containers for portside inspection. The system allows the container to receive a remote preliminary inspection without the container leaving the marine terminal.

By maintaining a record of each container's contents, the port is able to provide government authorities with a forensic tool that can aid a follow-up investigation should a container with a weapon of mass destruction still slip through. This tool would allow authorities to quickly isolate the point in the supply chain where the security compromise took place, thereby minimizing the chance for a port-wide shut-down. By scanning every container, the marine terminals in Hong Kong are well-positioned to indemnify the port for security breaches. As a result, a terrorist would be unable to successfully generate enough fear and uncertainty to warrant disrupting the global trade system.

This low-cost inspection system is being carried out without impeding the operations of busy marine terminals. It could be put in place in every major container port in the world at a cost of $1.5 billion, or approximately $15 per container. Once such a system is operating globally, each nation would be in a position to monitor its exports and to check their imports against the images first collected at the loading port.

The total cost of third-party compliance inspections, deploying "smart" containers, and operating a cargo scanning system such as Hong Kong's is likely to reach $50 to $100 per container depending on the number of containers an importer has and the complexity of its supply chain. Even if the final price tag came in at $100 additional cost per container, it would raise the average price of cargo moved by, say, Wal-Mart or Target by only 0.06%. What importers and consumers are getting in return is the reduced risk of a catastrophic terrorist attack and its economic consequences.

In short, such an investment would allow container security to move from the current "trust, but don't verify" system to a more robust "trust but verify" regime. That would bring benefits to everyone but criminals and terrorists.

Mr.Flynn is the Jeane J. Kirkpatrick senior fellow for national security studies at the Council on Foreign Relations and author of America the Vulnerable *(HarperCollins, 2005).*

Contents page available in eSS journals section.

Log on to : http://www.feer.com