

Safe Ports: A global Issue?

Donald C Masters, Ph.D. is a veteran U.S. Foreign Service Officer who spent most of his career overseas. Dr. Masters also worked for the World Bank (IBRD) specializing in development economics and public finance. More recently, he was senior consultant for International Development Business Consultants (IDBC) and adjunct professor of economics at the Monterey Institute of International Studies (MIIS). Currently, he serves on the HLSIA Board of Directors.

The nation's seaports reflect the dynamism of an open economy. Roughly twenty percent of U.S. national income is derived from merchandise trade. More than ever, the *inter-modal* shipping container dominates port commerce. There are an estimated 108 million cargo containers in circulation worldwide. Since these containers are used in multiple ports-of-call; this translates into a container-port throughput of some 500 million per year. According to U.S. Customs and Border Protection, roughly 90 percent of the world's manufactured goods are moved in shipping containers. This humble "steel box" has revolutionized the international transport system by providing a convenient *unit of conveyance* that is easily transshipped from one transport mode to another i.e., ship to truck or rail and vice versa. This relatively simple but highly efficient method of inter-connected transport systems has led to significant reductions in international shipping costs. For the U.S. economy, the overall average cost of freight shipment is equivalent to less than four percent of the total value of merchandise trade. Thus, technological advances in the transport sector along with tariff reductions, under the auspices of the World Trade Organization, have removed most of the physical and political barriers-to-trade. This permits greater *specialization*, based on cost competitiveness, with the result that an impressive array of manufactured products are now produced and assembled "globally". That is, production processes are dependent on components or sub-assemblies that are internationally outsourced and must be delivered on time. Similarly, the distribution of final product is destined for multiple national markets reflecting differing consumer tastes and local regulations. The resulting shift in world production patterns and related distribution of incomes has sparked controversy in some quarters. However, the dynamic benefits of trade are closely associated with economic growth and improved consumer welfare through lower prices and greater choice. The efficiencies associated with global specialization inevitably lead to increasing *interdependence*. This poses certain vulnerabilities which could be exploited by terrorist groups. The security challenge is to protect the nation from terrorism without unduly restricting the flow of international commerce.

Threat Scenarios

There have been a number of "war game" exercises to evaluate the economic impact of a major port closure due to a successful terrorist attack. These exercises usually take the form of a particular scenario which is based on a series of assumptions regarding terrorist intentions, capabilities and specific vulnerabilities of a major U.S. seaport. One such exercise focusing on the Port of Los Angeles/Long Beach estimated that the direct and indirect economic costs could

reach \$45 billion, under a set of plausible conditions.¹ This scenario envisaged the use of conventional explosives to destroy three bridges and one rail line connecting major port facilities i.e., Terminal Island to the rest of the port complex. Recently, public attention has shifted to a more sinister scenario, whereby a radiological dispersal device (“dirty bomb”) or a nuclear weapon is smuggled into a major U.S. port-of-entry. In such a scenario, the device would be detonated either in the port itself or in transit to an inland target. This has raised concerns about the possibility that the global supply chain could be used to convey a lethal cargo via the ubiquitous shipping container.

U.S. Response

Since 9/11, several important programs have been put in place by U.S. Customs and Border Protection. The *Customs -Trade Partnership against Terrorism* (C-TPAT) is a voluntary program enlisting major U.S. importers, carriers and shippers to strengthen security measures all along their supply chains. This includes overseas manufacturing subsidiaries as well as “outsourced” foreign suppliers. In exchange for “green lane” customs clearance, these private entities agree to enhance their security procedures. Currently, there are 6,000 C-TPAT participants of which, roughly two-thirds have been validated as fully complying with program guidelines. The *Container Security Initiative* (CSI) attempts to take security to foreign ports under reciprocal bilateral agreements whereby port authorities meet certain program standards and agree to inspect containers identified as “high risk” by a resident U.S. Customs and Border Protection team. This procedure depends on the cooperation of foreign customs services to inspect suspect cargos destined for U.S. ports. The so-called *24 hour rule* requires shippers and carriers to submit electronic cargo manifests at least 24 hours prior to ship loading at the foreign port. The electronic manifests are an important data source for the *Automated Targeting Center* whose algorithms identify which containers should be inspected. At present, fifty foreign ports are participating in the CSI program handling some two-thirds of U.S. containerized imports. Other programs include the DOE’s *Mega-ports program* which focuses on nuclear materials smuggling and most recently, the first phase of the *Secure Freight Initiative* which includes six foreign ports to provide radiological and nuclear screening for all containers destined for the U.S. market. Unlike the CSI program, the U.S. will supply the radiation screening equipment and establish alarm resolution procedures.

Safe Ports Act 2006

The Safe Ports Act strengthened key components of the CSI and C-TPAT programs by giving them legislative authority. It also expanded the Domestic Nuclear Detection Office (DNDO) authority to monitor port inspection procedures and acquire advanced radiation scanning equipment. In addition, the Act authorized higher levels of future fiscal year funding for port security grants (\$400 million). Furthermore, Customs and Border Protection was authorized to use “contractors” to review participant compliance with C-TPAT guidelines.

¹ See Chapter 3 “The Costs of a Terrorist Attack on Terminal Island” by Gordon et al., Protecting the Nation’s Seaports 2006, *Public Policy Institute of California*, editors Jon Haveman and Howard Shatz.

Significantly, it directed the U.S. Department of Homeland Security (DHS) to initiate a pilot program to test the feasibility of screening all containers bound for U.S. ports-of-entry (“Secure Freight Initiative”) and directed DHS to deploy enough radiation detectors to scan all containers in 22 of the nation’s largest and busiest ports by 2008.

Radiation Detector Performance and Deployment Issues

The current detection devices known as PVT (polyvinyl toluene) systems can detect radiation sources but cannot reliably identify whether the detected radiation is natural or man-made. Since many commercial products that enter the supply chain emit radiation, the current hand-held and radiation monitoring portals use a technology that is subject to a high “false positive” rate, i.e. presence of non-lethal radioactive material. The manpower requirements for more definitive inspections, either non-intrusive or physical, impose a heavy burden on Customs personnel and delay the flow of commerce. DHS has determined that up to a five percent “false positive” rate is acceptable. To stay within this threshold requires a new and more reliable detection technology, known as ASP (Advanced Spectroscopic Portal) systems. Since ASP detection equipment is considerably more expensive (roughly five-fold) than current PVT systems, the Government Accountability Office (GAO) which reports to Congress, strongly recommended that a cost-benefit analysis be done prior to planned procurement of “next generation” detection equipment totaling \$1.15 billion. The DNDO duly performed the GAO recommended cost-benefit analysis and proceeded to award a five year ASP contract to three vendors (Raytheon; Thermo Electron and Canberra Industries). The GAO in their October 2006 report to the Senate and House Appropriations Committee found the DNDO cost-benefit analysis to be deficient in a number of important aspects. The comparison of PVT and ASP costs and benefits was therefore seriously flawed and deviated from standard government cost methodology. The DNDO admits that the initial 80 ASP systems procured have not demonstrated that they meet the stated standard of accuracy i.e., 95 percent probability of detection. But DHS insists that the program must go forward and further testing (and calibration) will be conducted at New York terminals during the first year of the contract. A key element of this testing will be improvements in ASP software to achieve the desired level of accuracy. The DNDO deployment strategy contemplates a mix of ASPs operating in conjunction with PVTs with the latter serving as initial filters for radioactive substances. Hence, the main operational issue will be the optimal deployment mix of the two generations of technology and whether the layered security approach will yield an acceptable confidence level for the system as a whole.

Neither here nor there....

Meanwhile the new Democratic leadership of Congress is reportedly considering a 100 percent radiological scanning requirement for all containers destined for U.S. ports-of-entry. In practical terms this translates into the scanning of some 10 million containers annually, mainly at foreign ports, using technology that does not yet meet DHS performance specifications. That is, a “false positive” rate not more than five percent and ninety-five percent accuracy in identifying “masked” weapons grade material, such as highly enriched uranium (HEU). The current and

newer detection technologies would need to be substantially upgraded (and expanded overseas) in terms of the software driven analytical capabilities and their optimal port configuration. The Secure Freight Initiative at six newly selected foreign ports is meant to help determine whether full radiological screening is feasible, without massive backlogs of containers and their often time-sensitive cargo. Port simulation models may help in this regard. A key parameter is the 20 minute-per-container, non-intrusive scan time (using current gamma-ray and x-ray equipment) for the more definitive radiological inspections. This *flow rate* appears to be a significant operational constraint, given the number of containers to be scanned.

What seems to be emerging is a dual system to inspect containers and their cargos. The current programs (CSI, C-TPAT) rely on partial but targeted inspections, either overseas or at domestic ports-of-entry. With the Safe Port Act 2006, DHS is now directed to deploy radiation detection equipment and establish procedures that could eventually require radiological scanning of all containers destined for or entering U.S. ports. This raises a number of feasibility issues which will take time to resolve since they depend *inter alia* on international cooperation, improvements in detection equipment (speed and accuracy) and finally, availability of funding to build what essentially could evolve into a global port security program. During this transition period, it will likely fall to the *Automated Targeting Center* to keep track of the ten million containers that enter the U.S. every year in a way that avoids inspection redundancies and associated costs. Some suggested policy initiatives that might shorten this transition period are as follows:

Policy Considerations:

1. The U.S. should more proactively engage multilateral organizations to adopt reasonable and attainable *international standards* for detection equipment performance as well as procedures for their effective use. The US-EU Agreement signed in 2004 calls for greater regional cooperation with the CSI program. It established a working group consisting of representatives of U.S. Customs and Border Protection and the EU Commission and Member States to establish minimum standards for container “risk management techniques and related requirements...” This needs to move forward with an operational protocol that specifies port requirements that meet the mutually agreed upon standards for secure transatlantic trade. A regional consensus on equipment standards and port procedures could then be expanded through the World Customs Organization. That is, make operational the already existing 2005 agreement known as the “Framework of Standards to Secure and Facilitate Global Trade”. Alternatively, the U.S. could make use of other regional agreements, possibly under ASEAN or APEC auspices, with major Asian trading partners. Such negotiations will require patience and perseverance but if successful, they will make *trading partner countries fully responsible for the safety and security of their exports*. An offshore port security system will be far more cost-effective for the U.S. than the current patch-work of bilateral agreements involving the deployment of CBP teams and costly U.S. supplied equipment. Moreover, regional agreements that lead to internationally recognized

specifications and standards will *create a market* for security related equipment that is larger and more competitively organized than exists at present.

2. Open up the market for security equipment procured with public funds. Bid specifications should be as *source neutral and technology unbiased*, as possible. Detection performance should be based on objective criteria. For example, equipment that meets statistical standards such as a ninety percent confidence level (based on a “two-tail” test for Type I and Type II Error) might be the best approach. If preferences for a “national champion” are insisted upon, negotiate a preference rate of no more than say, 10 percent of bid price. International competition will still be possible and it will encourage country participation in the program. In the end, this will reduce the unit costs of equipment.
3. Encourage the use of commercially available dual-use technology to the greatest extent possible. This will also lower costs by allowing smaller firms to bid on contracts and it will encourage a *modular approach* in building security systems. Such an approach will make these security systems more flexible and responsive to evolving threats. Security concerns should focus on software integrity protection and not the hardware.
4. Encourage the timely sharing of information that detects anomalies in the supply chain. Port security is greatly enhanced if activity that occurs from point A to point B is passively monitored. There is an enormous amount of data that is generated by normal commercial activity. This background “noise” could be monitored with the help of advanced IT software to detect anomalies in the supply chain. This data set could then be further analyzed to determine if there is an “outside” threat. Private firms invest in *tracking technology* to improve logistics and related corporate decision-making. Currently, there are technologies, e.g. electronic seals on container doors and sensor-communication platforms being developed that have the potential of imbedding security-related features. However, the cost of these features cannot be of such magnitude that they cause the capital investment to become unprofitable.²
5. Finally, a wide range of technologies now exist that make *situational awareness* ever more feasible and available at reasonable cost. The effective use of these technologies requires integration. This must be based on the appropriateness of the system “architecture” i.e., enterprise needs in their particular commercial environment. As firms gain experience with the newer technologies, they will be able to respond to events with much greater alacrity. Should an anomaly occur that is suggestive of a terrorist activity, there needs to be in place a channel of communication with the appropriate government authority and a mutually agreed protocol for further action.

masters@hlsia.org

² See Chapter 5, “Harnessing the Trojan Horse” by Jay Stowsky, Ibid.