**Maritime Security**
Domain Awareness Defined

**Safety Enhancements**
Passive, But Critical

**Marine Coatings**
Spray on the ROI

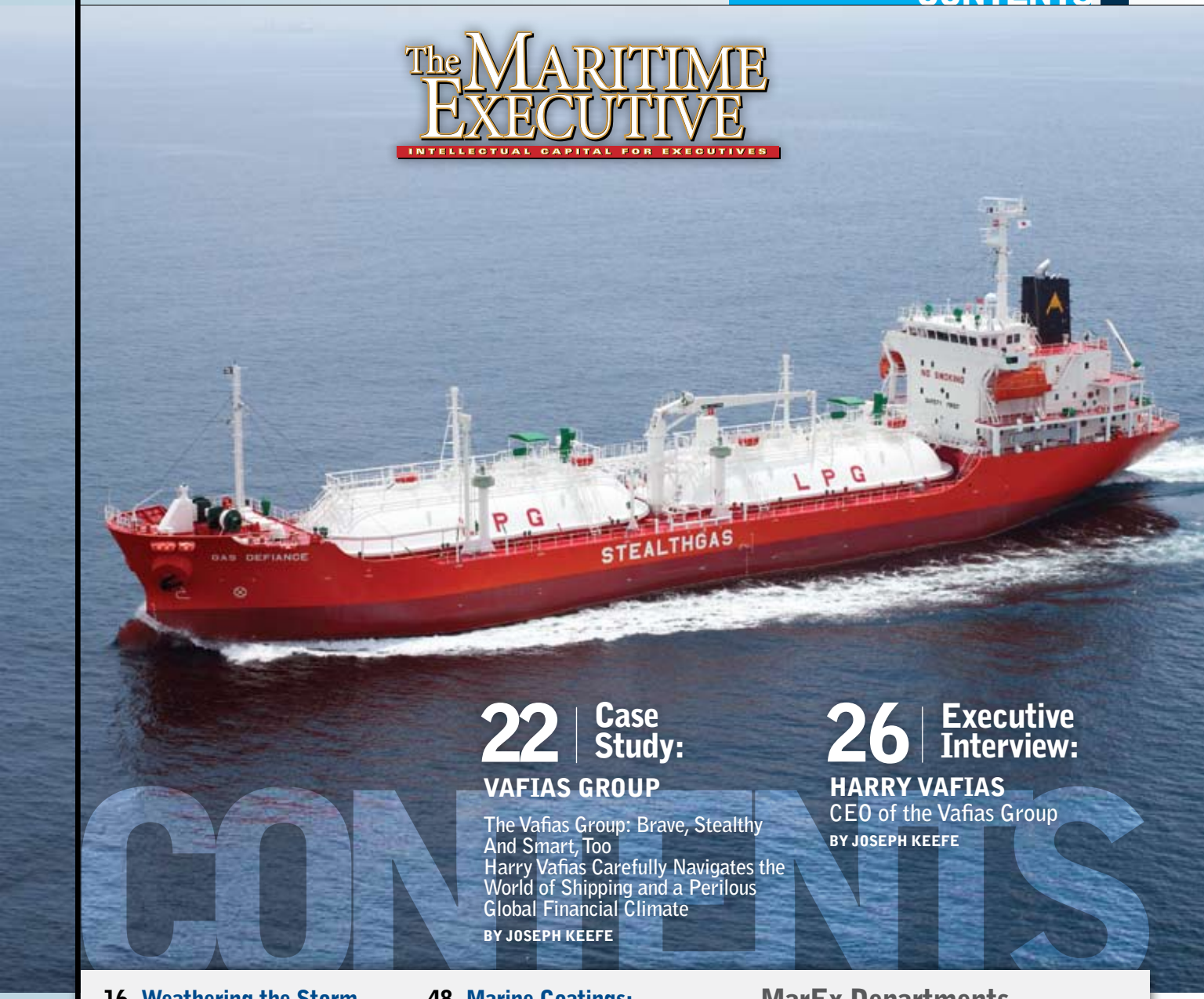
March/April 2009

# The Maritime Executive

INTELLECTUAL C[illegible] FOR EXECUTIVES


**Also in This Issue:**
Offshore LNG - Italian Style
Washington: New Energy Policy?

The Maritime Executive
INTELLECTUAL CAPITAL FOR EXECUTIVES




CONTENTS

By Dr. Jim Giermanski, Chairman, Powers Global Holdings

# SO YOU THINK CSI WORKS: Gummy Bears or Cocaine?

IN-BOUND CONTAINERS DESTINED for the United States are recognized as a vulnerability to our seaports. Yet, in reality, and contrary to popular perceptions, little is being done to diminish that vulnerability. There are three problems in dealing with this vulnerability: the accuracy of the Container Security Initiative (CSI) 24-hour manifest information filed with Customs and Border Protection (CBP); the accuracy and extent of use of scanning technology at CSI operational ports, and the transshipment gap.

## THE 24-HOUR MANIFEST

The first security weakness is the core component of CSI, the 24-hour manifest. A manifest is like a tally sheet of what the vessel is carrying. Except for visible cargo, the carrier has never known for sure what is in a locked and sealed container. The vessel carrier was forced to use honest terms like FAK ("Freight of All Kinds") or STC ("Said to Contain"), which accurately explained that this or that was supposed to be in the container. The reality is no different today under CSI, except that the carrier cannot use those phrases. The carrier must put on the manifest what the shipper or his agent says the contents are. In essence, nothing has really changed.

The purpose of the Container Security Initiative was to develop partnerships with foreign authorities to identify high-risk cargo containers originating at ports throughout the world before they are loaded on vessels destined for the United States. The CBP mandate is clear: "Carriers and/or automated NVOCCs (Non-Vessel Operating Common Carriers) will be required to submit a cargo declaration 24 hours before cargo is laden aboard the vessel at a foreign port for any vessel

beginning the voyage on or after Dec. 2, 2002." Unfortunately, the carrier makes and files the manifest and, as usual, is 100 percent dependent on the shipper (consignor) or the shipper's freight forwarder for the information about contents. As such, the vessel carrier serves as a third party in verifying the contents of the container, the equivalent of hearsay.

## Scanning Effectiveness and Accuracy

The second security weakness is the scanning itself. In referencing the requirement to scan at foreign ports, the 9/11 Commission Act of 2007 says that scanning "...shall apply with respect to containers loaded on a vessel in a foreign country on or after the earlier of--(A) July 1, 2012; or (B) such other date as may be established by the Secretary under paragraph (3)." (Section 1701)

Congress is expecting that new portal machines, or crane-mounted machines, will be developed and commercialized to detect dangerous radiation. The GAO -- in April of 2007 (GAO-07-347R, Combat Nuclear Smuggling) -- stated very clearly that the Domestic Nuclear Detection Office (DNDO), established and responsible for ASP (Advanced Spectroscopic Portals) development, has not even collected all the testing data on its basic PVT (polyvinyltoluene) portal detectors and is not close to any developed ASP portal detector. Experts do not expect a commercial version of the ASP anytime soon, if ever. There are no machines now, nor is it likely that there will be any in 2012 as required by Congress. Therefore, Congress allowed for an extension until such time as these radiation portal detection machines become available.

In any event, to focus on the discovery of a nuclear or dirty bomb arriving at our seaports is fundamentally flawed. It's too late if they are found at our ports. In fact, a detonation at our ports is likely to have a more deleterious impact nationally than a detonation within the interior of the United States.

Additionally, there are few foreign scanning programs. One is the Secure Freight Initiative (SFI), a scanning project composed of radiation portal monitors to detect radiation through NII ("Non-Intrusive Inspection") imaging systems. The Secure Freight Initiative is active at only three ports at full capacity: Puerto Cortes, Honduras; Port Qasim, Pakistan; and Southampton, United Kingdom, as opposed to the 58 foreign ports participating in CSI. At one time, it was active in a limited capacity at Pusan, Korea; Singapore; Port of Salalah, Oman; and Hong Kong. However, because there are significant problems with the SFI project, further deployment of machines is being reviewed.

NII imaging is really intended for small package discovery and border-crossing functions. NII is mobile gamma-ray imaging technology, which permits officers to quickly "see" inside tankers, commercial trucks, cargo containers and other conveyances without having to physically open the conveyance and/or container. NII machines can scan

vehicles up to 125 feet in length in one pass. One version of the system is mounted on a truck chassis and is operated by a three-man crew. The NII operates by slowly driving past a parked vehicle with a boom extended over the target vehicle.

CBP knows that scanning is a problem. It doesn't work well, and the CBP statistics on scanning are often flawed. It is common knowledge that hits by drug dogs that actually find the drugs cause the container to be consequently scanned. The scanner, then, gets the credit for the discovery, not the dog. CBP insiders have admitted that there are U.S. ports where there has never been a discovery by scanning. Instead, random inspections, informant information, and the dogs have actually been the source of discovery. Speed of movement through the portal machines, the distance of the radiation sensor from a source of radiation, and the capacity to shield radiation and hide drugs and human cargo hidden within and among other cargo simply make scanning a very poor, if not useless, process of law enforcement.

## The Transshipment Gap

The third security vulnerability involves transshipment. Historically, transshipment meant to transfer cargo for further transportation from one ship or conveyance to another. However, CBP considers transshipment as sending an exported product through an intermediate country before routing it to the country intended as its final destination. Specifically, transshipment means that the cargo does not arrive on the vessel it was laden into. So how does this arrival and discharging of cargo in the United States from a vessel different than the one that debarked from a foreign port impact U.S. security?

Under CSI, high-risk containers receive security inspections, including X-ray scan and radiation scan before being loaded onboard vessels destined for the U.S. Once high-risk containers are scanned at CSI ports, they are not scanned again until arrival at the U.S. seaport. Worldwide, there are 16 major transshipment ports: Singapore, Hong Kong, Shanghai, Kaohsiung (Taiwan), Pusan (Korea), Tanjung Pelepas and Klang (Malaysia), Rotterdam, Dubai, Gioia Tauro (Italy), Algeciras (Spain), Hamburg, Salalah (Oman), Colombo (Sri Lanka), Port Authority of Jamaica and Antwerp.

While not classified as major, there are many more in the Caribbean and South Atlantic, which are of special interest to the United States: Colon and Manzanillo (Panama), Cartagena and Barranquilla (Colombia), Pt. Cabello (Venezuela), Kingston (Jamaica), Havana, Cristobal and Balboa (Panama-Pac), Rio Haina (Dominican Republic), Bridgetown (Barbados), Pointe-a-Pietre (Guadeloupe), Vieux Fort (St. Lucia), and Point Lisas (Trinidad).

So what happens when a container is scanned in Japan but goes to Panama where it is discharged and placed in the port until it can be once again laden onto another smaller

container vessel for entry into the United States? It is not rescanned since many of these smaller transshipment ports do not have scanning equipment. Additionally, while there are CBP authorities at CSI-operational ports that are also transshipment ports, they are subject to the law of the country in which they were placed and may not personally check or inspect these containers even with intelligence that they contained drugs, counterfeit materials or explosives.

## THE OBVIOUS CONSEQUENCES

1 **The CSI 24-hour Manifest –** On December 29, 2008 CBP Field Operations officers in Port Newark discovered over 525 pounds of cocaine bundled inside duffel bags in the back of a container that originated in China and transited through Panama. Earlier in October, 330 pounds were also found in Port Newark. The combined estimated value was $42 million. How did this happen? In the December shipment, the CSI 24-hour manifest listed silicone solar cables and other equipment destined for California. In the October shipment, the manifest said the container carried gummy candy. It is quite clear from this that relying on a third party's knowledge of contents is utter foolishness. Hopefully, the 10 + 2 Rule that went into effect on January 25, 2009 will fix the obvious weakness in the 24-hour rule, since the 10 + 2 Rule places the onus for content identification rightfully on the U.S. importer and his agents and/or business partners. Yet the same weakness is still present at the border crossings into the United States where there is no 10 + 2 Rule, and a third party enters contents about which he knows nothing into the Automated Commercial Environment (ACE) System. The manifest has historically been and should remain a carriage document, not a security document.

2 **Scanning –** Presumably, these shipments were scanned in China. If they were, only one conclusion can be made. The scanning didn't work. If the scanning worked, then there were no drugs in the container at the time of scanning. Inside CBP personnel confirm that even if the drugs were in the container, the scanning would likely not discover them. Additionally, CBP has confirmed in the case of Port Newark that information they were given triggered the inspection, not a scan. So if the drugs were not in the container in China, when did they enter the container? Again, options are quite limited but obvious. In all probability, the drugs were put into the container in the transshipment port in Panama from which the transshipped container came.

3 **Transshipping –** So what would you do as a terrorist? Ship directly, or ship through a small recognized transshipment port? Transshipping is the greatest threat to the port security programs of the United States.

Transshipping is not only a means of entering smuggled and counterfeit products but also weapons of mass destruction (WMD). No manifest or worldwide scanning can fix it. Just like the drop lots along the Mexican border, terrorists and smugglers have almost unfettered access to containers and trailers waiting for pick-up and movement into the United States. Imagine what could happen if the 855 pounds of cocaine were 855 pounds of high-grade explosives. Now pretend that these explosives were in a container with an RFID (Radio Frequency Identification) tag. Knowing that an RFID tag can serve as an improvised explosive device (IED), it doesn't take much further pretending to visualize the result, a real shut-down of all our seaports and land ports with disastrous economic consequences.

## CONCLUSION

There is only one fix. The largest global port terminal operators know what it is. China knows. The EU knows. And now even Mexico knows. The only answer to this vulnerability is the use of container security devices (CSDs) that in real time trace and track containers from stuffing to unloading. Smart containers can provide an electronic chain of custody that does the following:

1 Employs a system approach to coordinate all facets of the supply chain process, beginning at origin, by identifying and recording the person responsible for supervising and verifying contents at "stuffing" and securing of the container at the foreign point of origin;
2 Links electronic trade data to other documentation, like container number or booking number, trucking bill of lading information and even portions of the Inward Cargo Declaration, Customs Form 1302;
3 Detects and reports in real time with date, time and geographic location of the breach anywhere into its body, not just through the doors;
4 Gives its geographic position throughout the supply chain when queried, or automatically give its position if it is off its designated course of travel;
5 Recognizes and records the identity of the authorized person opening the container at destination; and
6 Uses different sensors and communicates with or adapts to divergent logistic software packages used by shippers and carriers within the supply chain.[1]

All this is known except in the United States where we still rely on CSI. So why is it that the U.S. doesn't know? CSI is not the solution. It might even be the problem, especially in light of the transshipment vulnerability, which allows gummy candy to be something else. The only thing worse than the transshipment vulnerability is not knowing how to fix it. ***Mar***Ex

*1 James Giermanski, "Boxing Clever," Cargo Security International, Vol. 4, No. 1, February/March, 2006, p. 44.*

**Dr. Jim Giermanski** *is Chairman, Powers Global Holdings, Inc., an international transportation security company. A reviewer for the Transportation Research Board, U.S. National Research Council, and past Director of Transportation and Logistics Studies, Center for the Study of Western Hemispheric Trade at Texas A&M International University, he is frequently invited to testify before the U.S. Senate and House, EPA, and U.S. International Trade Commission. He sat for 5 years on the Texas Office of the Attorney General's Trans-border Trucking International Working Group, as well as being a member of the Research Advisory Committee on Management and Policy, Technical Advisory Panel, Texas Department of Transportation. He has been published extensively on transportation and trade issues. His background includes service as an FBI special agent, Colonel, and Special Agent in the Air Force Office of Special Investigations.*