US Port Security – Seaport Security Starts Far from Home

The United States' maritime strategy states that homeland security begins as far from home as possible. Port security in the US starts where the containers are loaded abroad. *Edward Lundquist*, retired US Navy captain, explains how good law enforcement comes from good relationships

An LRAD Corporation acoustic device combined with a FLIR imaging sensor – a powerful fusion of sound and vision

The United States' *A Co-operative Strategy for 21st Century Seapower*, which was signed by the service chiefs of the Navy, Marine Corps and Coast Guard, recognises that preventing wars is as important as winning them. Maritime security is now a core priority of all three sea services, and the strategy acknowledges that maritime security at home depends on maritime domain awareness on all oceans. Secure ports at home begin with trading partners abroad.

The vast majority – more than 90 per cent – of global trade is conducted on the sea, so maritime security isn't just a problem for seafaring nations. "It's more than just maritime nations that are affected by protection of the global commons – it's essentially the world," says Mark Andress, director for US Navy Maritime Domain Awareness. Because of this, he says, "We have been actively focusing on fostering an environment where global maritime safety and security are a priority."

He says that the navy cannot collect and process all the information by itself, but relies on interagency co-operation and regional partnerships led by foreign countries in their region. "Our strategy is about establishing trust and sharing in a region. By establishing these sharing networks, you're also better able to respond at times of crisis. You've got a known group of people that you can reach out to for other information. Often, those barriers to sharing information may exist on a day-to-day basis, but during a crisis these barriers suddenly shift, and information starts pouring more freely to help address a certain issue."

"We have a group of international officers here on the staff who are committed to seeking ways to communicate with our partners throughout the region more effectively," says Rear Admiral Vic Guillory, US Navy, who is Commander of the US Fourth Fleet and Naval Forces Southern Command (NAVSO). "We host an Inter-American Naval Telecommunications Conference (IANTN) where we work on both hardware and other agreements to allow us to communicate better, to share information and to understand more about the maritime environment in the SOUTHCOM region, and to enhance everyone's awareness of what's just beyond the horizon."

"Our strategy is about establishing trust and sharing in a region"

The International Ship and Port Facilities Security Code

With so many shipments coming to US shores from overseas ports, it is imperative to ensure the cargos and vessels have not been compromised at any time. After 9/11, the International Maritime Organisation (IMO) amended the 1974 Safety of Life At Sea (SOLAS) Convention to include new 'Special Measures to Enhance Maritime Safety'. These include the International Ship and Port Facilities Security (ISPS) Code, which requires governments to carry out security assessments to "identify and evaluate important assets and infrastructures that are critical to the port facility as well as those areas or structures that, if damaged, could cause significant loss of life or damage to the port facility's economy or environment". It provides a framework for governments, agencies and the shipping industry for conducting risk management between potential threats and the vulnerability of ships and port infrastructure. Furthermore, the US Maritime Transportation Security Act of 2002 (MTSA) requires that anti-terrorism measures be assessed in foreign ports that receive vessels due to call on the US.

The Coast Guard's International Port Security (IPS) Program involves several dozen Coast Guard officers who assess port security measures in thousands of ports. The Coast Guard began conducting the port security assessments in 2004. While these officers are evaluating compliance with regulations, they are also conducting valuable person-to-person engagements in these ports, and this can lead to capacity-building opportunities. IPS officers assess the effectiveness of anti-terrorism measures in foreign ports to ensure that a foreign port has adequate anti-terrorism measures, and help those appropriate authorities to improve their anti-terrorism posture, which in turn can reduce the security risk to the US from vessels that arrive from those ports.

"We attempt to visit the country to observe the security conditions, and we only inspect the ports of countries that have maritime trade with the US," says Lieutenant Commander Tanya Schneider, a Coast Guard International Port Security Liaison Officer. "We meet with the people who are responsible for port security in those countries and at those ports, and we ensure that the port complies with international security regulations."

Another way to provide port security at home is to ensure that appropriate measures are taken at the point of cargo loading. The Container Security Initiative (CSI) allows US Customs and Border Protection (CBP) agents, along with their host-nation counterparts, to examine high-risk maritime containerised cargo at foreign seaports before it is loaded onto vessels destined for the US. According to the US Department of Homeland

Ear biometric systems will make it harder for undesirables to pass through undetected

Security (DHS), 58 foreign ports, accounting for 85 per cent of US-bound container traffic, currently participate in CSI.

Learning lessons from the USS *Cole* attack

In the year leading up to the 10th anniversary of the attack on USS *Cole* (DDG 67), the US performed an extensive navy anti-terrorist/force protection (AT/FP) programme assessment, which included tabletop and operational exercises, fleet-wide interviews and administrative reviews. While deployed and deploying units have embraced lessons from the *Cole* attack, the freedoms and the nature of America's open society create potential vulnerabilities at home ports. New technologies, including non-lethal systems, can both monitor port areas and warn potential threats to stay clear. The networking of acoustic devices with remote-sensor systems permits real-time communication and response. "Directed long-range acoustic tools ensure instructions are heard and understood, greatly helping to reduce miscommunication and confusion," says Scott Stuckey, Vice-President for Business Development for LRAD Corporation, which makes the Long Range Acoustic Device (LRAD).

"Sounding alarms, using laser dazzlers and firing flares can help get a boat's attention. An acoustic hailing device's intolerable sound can compel a suspect vessel's crew to turn away," Stuckey adds. "The LRAD can transmit a powerful directed warning tone up to three kilometres away. This tone can be followed by clear, highly intelligible communications in the appropriate language, warning suspicious craft to keep their distance. If the suspect boat continues to approach, a crew can presume the intent of people on the boat, and escalate force-protection measures."

Detecting dirty bombs

Ports must remain vigilant against the arrival or transfer of materials that could pose a threat, as stevedores move the containers from the ships to the dock so that teamsters (truckers) can deliver them to their next destination. The trailers and chassis are scanned by Customs and Border Control for radiological and other hazards using radiation portals and other sophisticated equipment to inspect cargo and scan containers. Mobile radiation portal monitors screen containers for nuclear and radiological materials, and large-scale, non-intrusive X-ray equipment can scan an entire container within two to three minutes.

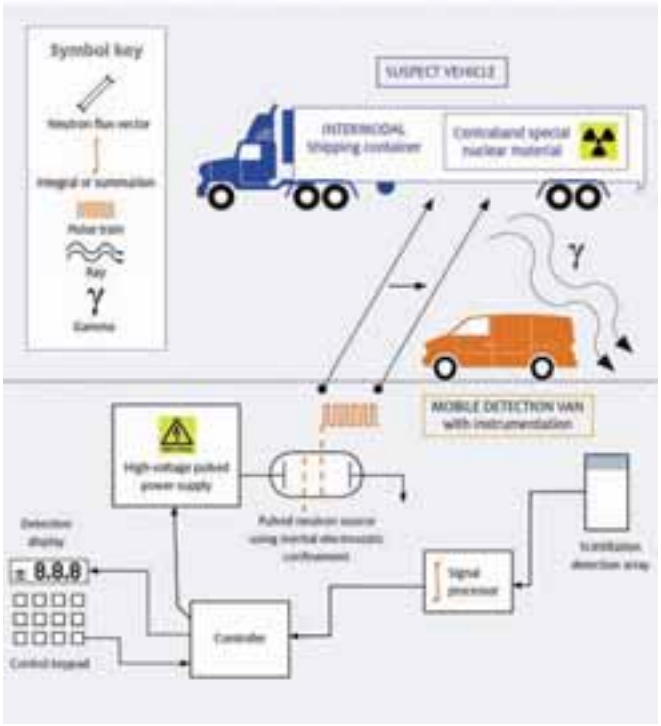
Furthermore, drive-through scanning equipment allows officials to detect suspicious or contaminated shipments. "Intermodal containers are ideal platforms for terrorists to place high explosives and chemical, biological nuclear or radiological weapons (CBRN) agents and devices and deliver them directly to any North American target," says Bradley Boyer, CTO of Petradyne Research Corporation. "A terrorist's nuclear weapon could be fabricated in most machine shops by hand-operated equipment, with a little surplus military gear – such as an old artillery piece – and other commercially available materials, within one year if the enriched uranium was available."

To counter this treat, the company is developing the Activation of Radiation, Gamma-Uranium Sensor (ARGUS) system for detection of nuclear materials via covert and mobile detection methods. The neutron pulse burst that the system emits penetrates the metal of intermodal containers that blocks X-ray-based equipment.

Keeping out the bad guys

Identifying known suspects can be a crucial piece of information, but a definitive way to uniquely identify people has, until now, been virtually impossible. This is where biometrics plays a role. Systems that use biometric measurements were successfully demonstrated during Green Devil II,

Graphic explaining how the Petradyne Research Corporation Argus system looks for nuclear material in a passing cargo container



a collaborative effort between the Marine Corps Systems Command (MCSC) and the Office of Naval Research (ONR), conducted at Fort Huachuca, Arizona, last summer.

Green Devil II demonstrated how different sensors can be used to increase situational awareness in the battlefield environment by collecting, fusing, transporting, analysing, delivering, exposing and acting upon data, and – most importantly – how to get real-time data to the expeditionary forces on the ground that need it. However, the technology can also be applied to infrastructure protection or port security.

"Facial recognition is considered hard biometrics," says Dr Mary Ann Harrison of the West Virginia High Technology Consortium (WVHTC). "We can distinguish between identical twins with a high level of confidence. Beards, changes in facial hair or hair colour, or make-up, do not matter."

Ear biometrics was also used during Green Devil II. The Ear Recognition System is a new capability developed by WVHTC with ONR support. Every person's ear is unique. It can confirm identity, and can also be observed at a distance.

In addition, new 'subscribable' systems make vetted intelligence available immediately to individuals who have 'subscribed' to information within specified parameters. "A person who is 'watch-listed' can be identified at a tactically significant distance," says Martin Kruger, an Intelligence, Surveillance and Reconnaissance (ISR) Program Officer at the Office of Naval Research. "We can provide this information quickly to people who need it, with a high level of confidence."

Sea ports represent not just a prime target for attack, but also the means for infiltrating personnel and materials into the country. The US has invested time and money to stiffen its defence against the use of its coastline for illegal acts. Europe, too, has implemented the ISPS Codes and installed equipment to search out suspicious cargo. However, the question that remains is what are the terrorists themselves are doing in the meantime to counter these efforts. ■