



CARGO SECURITY

INTERNATIONAL

www.cargosecurityinternational.com

Volume 7 Number 6

December 2009 / January 2010

Inside:

- Fleet Management
- Container Tracking
- TAPA Update
- Model-Based Risk
- Conference Diary

WATERSIDE SECURITY: What lies beneath?

Safe harbour

In the first of two features on port security, Lesley Bankes-Hughes looks at how US policy makers and port stakeholders are working to reduce the vulnerabilities of the waterside sector within the port environment

At a recent port security conference in Barcelona, Christian Dupont, Deputy Head of Unit, Maritime Security, **European Commission (EC)**, spoke of his concerns about the issue of waterside security within the port environment. While policymakers and port and terminal operators continue to be exercised by the problems of access controls, credentialing, and cargo scanning within the landside sector of a port, Dupont complained that taking cohesive action to protect the seaward side remained a low priority on most security checklists – in spite of the fact that events such as the attack on the *USS Cole* in Aden in 2000 and the 2008 Mumbai bombings have already demonstrated the obvious vulnerability to attack from this side of a port.

‘Let’s be frank,’ said Dupont, ‘there is no real mandatory provision about the waterside.’ The *International Ship and Port Facility Security (ISPS) Code* does touch on the issue ‘but in a very restricted way,’ he said, through the requirement for waterside patrols. Speaking on behalf of the EC, Dupont noted that: ‘It is certainly our intention to address this when we undertake a complete recap of our maritime security regime.’

Other speakers at the conference acknowledged that there was an imperative for action on waterside security. Capt. John Koster, Commanding Officer, **US Coast Guard (USCG) Activities, Europe**, agreed that this was an area for concern ‘even in developed countries’, while Juan Martin, Security and Safety Manager at the **Port of Vigo**, in Spain, admitted that measures such as the better deployment of divers to survey cruise ship berths should be considered. ‘We should increase this, but we are reactive – a law appears and then we follow.’

The difficulties of establishing safe waters and maintaining adequate surveillance methods are self-evident. The deployment of sonars, camera surveillance systems, divers and seabed mapping can, if properly integrated, create an efficient security ‘web’, but

the sheer scale of day-to-day legitimate traffic within port waters, including pleasure craft, fishing vessels and bunker barges, makes spotting anomalies a labour intensive – and, of course, costly – procedure.

The ISPS Code requires port operators to implement a security plan but it is not prescriptive about what the measures should be, or indeed how the parameters of a port facility are actually delineated.

In the United States, the *Maritime Transportation Security Act (MTSA)* of 2002 (and implemented through 2003/2004) can be seen as the initial driver behind a concerted attempt by over 330 national commercial ports to revise and improve their security programmes. This Act enshrined and mandated the security requirements contained within the ISPS Code and the 2002-amended *International Convention for the Safety of Life at Sea (SOLAS)*. Amongst other things, it required port authorities, terminal and facility operators, and state and local government agencies to act together in devising *Area Maritime Transportation Security* plans.

The *Port Security Grant Program* has also been established to provide some \$150 million in *American Reinvestment and Recovery Act (ARRA)* stimulus funding with seven ports labelled as requiring the highest level of security (Group 1) and 48 facilities classed as a slightly lower risk category (Group 2).

Back in 2003, as the implications of the MTSA were beginning to be realised, Admiral Thomas H. Collins of the USCG gave testimony before the **Committee on Commerce, Science and Transportation**. He acknowledged that the cost to industry of implementing MTSA regulations could be some \$1.5 billion in the first year and around \$7.3 billion over the next 10 years. Significant expenditure indeed, but these figures can perhaps be put into context when considered alongside the estimated \$58 billion cost to the US economy of a maritime terrorist attack.

Within a US port environment, responsibility for waterside security is shared between the port operators,

'The application process for funding may be cumbersome, time consuming, and brings with it its own cost burden'

government agencies such as the USCG, **Customs and Border Protection (CBP)**, federal police forces, and terminal operators. While responsibility for the procurement of security systems such as surveillance cameras primarily rests with the individual port authority, the USCG is heavily involved with measures such as port water patrols and plays a key role in coordinating the security tasks of the various interested organisations. These agencies are usually coordinated by an **Area Maritime Sector Committee** (also called a coast guard sector) which will often be chaired by a senior USCG member.

With maritime domain awareness (MDA) as one of the keystones of its operations, the USCG takes on responsibility for the enforcement of fixed security zones and patrols maritime approaches, the coastline, ports and inland waterways of the United States. Cutters, helicopters and shoreside patrol boats are all used to maintain surveillance of the waterside port area, and one of the major functions of this agency is the capture and dissemination of intelligence garnered from sources such as maritime intelligence fusion centres and vessel tracking systems such as the *Automatic Identification System (AIS)*.

The USCG has also addressed the problems of waterside security through the establishment of initiatives such as the **Underwater Port Security Working Group** which looked at issues such as the need to inspect vessel hulls, piers and bulkheads as well as improve the mapping of the seabed. The detection of

anomalies such as Improvised Explosive Devices (IEDs) within port waters as well as the interception of unidentified swimmers and divers were also flagged up as problems to be tackled within the risk assessments undertaken by individual ports. The USCG's research and development (R&D) capabilities have also been channelled into devising anti-terrorist measures such as anti-swimmer systems, underwater loud hailer and non-lethal weapons such as guns which use high pressure air jets. USCG partnership with **US Navy R&D** efforts has also proved fruitful in combating the offshore threat, and also independent naval research and pilot programmes are often used as the testing ground for the development and testing of commercial technologies such as sonar systems and seabed mapping.

In an ideal world, every US port would be able to implement a comprehensive range of above, on, and below water security measures which would be interconnected and monitored by means of a seamless systems integration solution. In practice, each port has to make a pragmatic threat assessment and decide what really are the essentials on its equipment wishlist. However, where US ports do have the financial advantage over European ports, for example, is the access to federal and state funds for equipment procurement. While the application process for funding may be cumbersome, time consuming, and brings with it its own cost burden, the fact is that money for security measures is available in the United States whereas in other parts of the world the issue of cost is frequently a problem which weighs heavily on the shoulders of port and terminal operators. Decisions made outside the United States on equipment procurement are therefore often predicated on issues of system multi-functionality as much as an overriding focus on their security applications.

The availability of port security grants and federal research and development money for pilot initiatives can also be seen as one of the reasons why many global product manufacturers seem

to perceive the United States as the primary location for systems testing and development whether it be by government agencies or by individual port operators.

As would be expected from the second busiest port in the United States, the **Port of Long Beach (POLB)** has a complex and wide-ranging waterside security strategy. For example, in June this year the POLB's **Board of Harbor Commissioners** gave the go-ahead to **Kongsberg Defence and Aerospace** for the delivery of its C-Scope underwater surveillance system which will provide a state-of-the-art automated detection and response capability for small craft, swimmers and divers.

However, while individual and invariably very expensive items of equipment play a valuable part in waterside security, their true potential as countermeasures is best realised as part of an integrated security strategy rather than as a stand-alone defence. Many US ports now have their post-9/11 security measures in place and are therefore beginning a process of evaluation of those earlier, sometimes *ad hoc*, strategies. Out of this process is developing a recognition that joined-up thinking is needed in the operation of individual security measures, and data collection from a number of information streams must form part of intelligence sharing not only at state level, but must feed through to national, international and multi-agency platforms.

At POLB, a \$21 million Joint Command and Control Center has just been opened which brings together local, state and federal security agencies, such as the **Los Angeles Police Department (LAPD)**, CBP, USCG and all the Port's security operations. **Activu Corp.** has developed and provided what it calls an IP-based 'visualisation and collaboration' solution for this command and control centre which allows the shared viewing and dissemination of information. According to the company, the system was deployed within a three-month period, and a similar solution has also been deployed at the **Port of**

Charleston. The proximity of POLB to the **Port of Los Angeles (POLA)** means that the two ports have a close dialogue on many matters, including security, and while the POLB Command and Control Center will in the near term operate independently of POLA, a spokesperson for Activu said that two POLA security officers will be stationed in a room adjacent to the main command centre.

It is the scaling-up of information sharing which Jay Grant, Director, **Airport and Seaport Police, USA**, sees as critical to a multi-layered approach to port security. Speaking at the Barcelona conference, he provided details of the *Security Resources Management Exchange (SRMX)*. This US Airport and Seaport Police project is a secure but easily usable internet platform where data about environments such as ports can be accessed by, and receive input from, national and multinational agencies so as to create more accurate threat assessments and pinpoint weaknesses in the US and global security web.

POLB's next door neighbour, POLA, has a similarly proactive approach to the issue of waterside security. George Cummings, Director of Port Security at POLA, rejects the view that this area of security receives scant attention: 'We take a layered approach to security, and waterside security takes up a large amount of our attention.'

As with POLB, waterside security is handled on a multi-agency level. The port police are drawn from the Los Angeles Police Department, and their numbers in recent years have grown from 65 to the current force strength of 135. Four patrol boats are deployed in port waters, there are frequent diver operations and a sophisticated camera surveillance system has recently been installed. In terms of information sharing and assessment, Cummings says that the port is looking to establish a joint protection committee which will link all the available information interfaces. Fibre optic projects are currently underway to create the appropriate network for

'We feel our customers do look at those ports which can protect their investments...while at the same time facilitating commerce'

the sharing of information and he says that the process of integration and commonality should be ready to go in 2010.

Cummings acknowledged the development of POLB's sophisticated Command and Control Center and suggested that at some point in the future POLA 'could probably hub with them'.

To date, POLB has received federal and state funding of around \$80 million in grant awards, but Cummings is keen to point out that much of equipment procurement at the port is based on a reimbursement basis whereby purchases are made by the port and then funding can subsequently be drawn down to meet the costs.

Cummings makes a pertinent point with regard to the availability of federal or state funding. While this money pays for the equipment, 'all operational and maintenance costs are borne by us,' he says. This cost burden is not inconsiderable and Cummings says that 'we are working with the federal grant committee on this and asking for a greater level of consideration about these follow-on costs'. POLA is also working with the **American Association of Port Authorities (AAPA)** to achieve some easing of this cost burden as, says Cummings, 'this is a problem which affects all US ports'.

POLA's new camera surveillance system includes some off-the-shelf equipment, says Cummings, but some of the technology 'is right up to the leading edge, and some of the software applications have been developed just for us'.

One of the potentially most useful initiatives instigated by the port is underwater mapping. The port police have worked with the port's maintenance teams to research and create a full set of baseline images. 'The federal government doesn't actually require us to do this,' says Cummings, 'but it is very valuable in picking up anomalies.' **Triton Imaging Inc.** secured the contract to undertake the seabed mapping at POLA using its *HarborSuite* data acquisition system to collect baseline information about the port which has a waterside area of some 7,500 acres, 70 kilometres (km) of channels, 17 recreational marinas, and 270 berths. John Thomas, Triton's programme manager, told *Cargo Security International* that the company is also currently working on baseline mapping at ports used by the US Navy.

Every US port addresses the issue of waterside security in the light of its own access to funding and equipment priorities as well as considerations such as vessel throughput and geographic factors. For **Port Freeport, Texas**, the 13th largest US port in terms of foreign cargo tonnage, the subject of port waters security was a key concern. In 2008, the port completed the implementation of a \$2.3 million waterside perimeter protection project. **Ciber Inc.'s Enterprise Security System Practice** integrated port security, port safety, MDA and port management systems into a single command and control solution. The port security system at Freeport includes features such as an integrated security system for video surveillance, intrusion detection and access control. 'Intelligent' radar systems are used for small-craft coverage and swimmer detection within the harbour. Large vessel tracking is undertaken within the harbour and up to 27 km outside it, while a base station has been set up to track AIS-equipped vessels within the harbour and up to 48 km outside its limits. Patrol boat tracking and a waterside perimeter intruder detection and alert system also form part of the port's security 'net'.

In October 2009, the port further

‘Each leg of the projects produced its own challenges which were met by a “can do” attitude and open communications with vendors and producers’

boosted its defences with the acquisition of a **Sonardyne Sentinel Intruder Detection Sonar (IDS)** and a deployment system for a fixed, permanent installation. The system, which protects vessels, port areas and waterside installations from intrusion by divers, swimmers or surface vessels, will be integrated into the port’s new command and control system.

Rick Benavidez, Director of Security and Safety at Port Freeport, told *Cargo Security International* that with the deployment of the Ciber and Sonardyne systems, ‘We now have landside, waterside and underwater detection systems...The Port’s financial investment in these security initiatives shows support for a “safe and secure Port”.’

Benavidez also makes the point that good waterside security also makes good commercial sense in today’s economic climate: ‘We feel our customers do look at those ports which can protect their investments, i.e., their cargo and vessels while at the dock, while at the same time facilitating commerce. Security is now synonymous with “asset protection”.’

George Cummings at the POLA made it clear that security projects have to be driven by the availability of state and federal funding, and Benavidez takes an equally realistic and practical approach: ‘One of our challenges was to complete this phased approach dependent upon funding. Each leg of the projects produced its own challenges which were met by a “can do” attitude and open communications with vendors and producers.’

The **Port of Portland**, Oregon, was one of the first ports in the world to specialise in intermodal container operations and its cargo throughput ranks it as the fourth busiest containerport in the United States. Its security assessment has resulted in considerable investment in access point security, scanning systems and the installation of hard perimeter fencing, including the procurement of waterside fencing at Terminal 4 funded by a \$220,000 federal grant.

Formerly with the USCG, Geoff

Owen is the port’s newly appointed Marine Security Manager. He notes that, to date, the port has not opted for equipment such as sonar detection or other underwater anti-swimmer systems. ‘We haven’t done any of that – the port has done a threat assessment and doesn’t think it needs it at the moment,’ he says.

However, the port has a camera surveillance capability which covers the entire pier face, and Owen says that in any future phase of the port’s security programme ‘we would be looking at an analytics capability that will allow the cameras to self monitor and issue alerts if something enters the field of view’.

As with the other quoted port security directors, Owen points out that obtaining funding is not without its difficulties. In terms of equipment procurement, there is often an element of fund matching, he says, and the amount given can vary to a significant degree depending on whether the source of funding is a private or public entity.

Owen also stresses that funding applications are not without attendant costs to the port itself and that the current economic situation has exacerbated this problem. ‘Nothing is free and grant applications can be complex,’ he says, adding that ‘some ports have hired staff simply to manage the grant process’.

He notes that there is still residual funding available in 2007 and 2008 federal allocations, where the fund matching requirements have been firmly stipulated, but he expresses a wish that ‘in the matching requirements for some of the later funding we might hope for a lessening – or a waiver – of some of the requirements’.

So while federal and state funding has been the real driver for the development of waterside security initiatives in the United States, the ability of a port to make its own financial contribution to projects is not without its difficulties. In the next feature, looking at waterside security outside the United States, the question of how ports can fund their ambitions for expensive security systems may be even more difficult to answer.