Analysing threats, policies and solutions in port security

Dr Angela Carpenter, *visiting researcher, University of Leeds, United Kingdom*

Port and harbour security became an issue of growing concern in the wake of the September 2001 (9/11) attacks on the US, the attacks on the naval destroyers USS The Sullivans and USS Cole while tied up in the Port of Aden in Yemen in 2000, and the French oil tanker Limberg in 2002. Prior to these attacks the main focus of port security was often directed at land-side threats such as the theft of cargo from containers, warehouses, or ships berthed in port. Securing perimeter fencing to prevent thieves from accessing the port area including warehouses was often the main concern, particularly in ports adjacent to urban areas. Similarly, there is potential for undocumented migrants to enter a port and attempt to stow away on ships, in containers or in trucks parked in the port area.

International policy response to 9/11 attacks

In the wake of 9/11 international measures were introduced by the International Maritime Organization (IMO) to provide greater protection from potential terrorist attacks on ports and on the ships using them. These measures included the International Ship and Port Facility (ISPS) code[i], a set of measures introduced in 2002 under chapter XI-2 of the International Convention for the Safety of Life at Sea[ii]. This establishes mandatory requirements on both ships and ports to enhance maritime security. Under the code, ports are required to have a port facility security assessment conducted by a recognised security organisation, which examines the physical security of the port, its structural integrity, personnel protection and also transport infrastructure such as access points for road or rail transport. Having identified potential security threats, a port facility security officer is responsible for maintaining a security plan for the port covering aspects such as who can access the port, how to identify individuals in the port area, and how to ensure the physical security of the port, including its buildings and infrastructure, from land and from sea. The security plan should also identify the relevant agencies to be contacted in the event of different types of security breach (local police, immigration officials, security forces or the military for example). In 2003, a code on practice in port security was introduced by the IMO and the International Labour Organization[iii] and this document outlines the security requirements placed on ports.

The introduction of the container security initiative (CSI) in 2002 required pre-screening of all containers destined for US ports, such as Long Beach (pictured), from participating foreign ports

Photo Courtesy of the Port of Long Beach

Container security initiative

Subsequent to the 9/11 attacks, the US introduced its container security initiative (CSI) in 2002 (see US Customs and Border Protection[iv]). This required pre-screening of all containers destined for the US from participating ports. These CSI operational ports include many of the largest container ports by volume of cargo, and from around the globe. The three main elements of the CSI are identifying high risk containers that pose a potential risk from terrorists, screening them before they depart for the US, and using technology to conduct that screening without causing any delays in the transport of the cargo. Screening by manual inspection, with the contents of a container emptied and examined by hand or even disassembled, is the most common way of inspecting containers for

contraband goods, while canine patrols may also be used to identify drugs or explosives. However, CSI ports have a range of non-intrusive methods available to screen a container including x-ray or gamma scanners to generate an image of the contents and identify whether any additional searches are needed, and also radiation detection devices to identify any radiological hazard. The result is that far fewer containers need inspecting manually and ships can be loaded more quickly. While expensive in terms of initial cost, such technology can prove a cost-effective investment towards improved security and faster throughput of containers.

Container security technology

While the vast majority of ports are not part of CSI agreements, developments to improve containers themselves may also prove beneficial. The introduction of technology such as high security mechanical seals, electronic seals, anti-tamper technology, and the use of global positioning system (GPS) devices are some of the recent developments to better ensure container security, both in port and at sea. There are also developments in the area of new materials to create lightweight, flexible containers, with embedded sensors in the walls, doors and floors which detect any breaches and transmit alerts to relevant agencies. Secure storage of containers in ports, with designated areas covered by motion detection, CCTV or other surveillance tools will also help better protect containers and cargos, while carbon dioxide monitors can be used to identify whether there are any stowaways hidden inside containers or in confined spaces on board ships.

Smuggling through ports

Smuggling by sea is an effective and lucrative way of transporting goods from one location to another, with drugs, tobacco and cigarettes, alcohol, counterfeit goods and undocumented migrants being smuggled on board ships. In addition, there are reported cases where weapons such as small arms and light weapons, explosives, anti-tank rocket launchers and anti-aircraft equipment have been smuggled on board ships. Drugs have been found concealed in cargos as different as concrete blocks, crates of bananas, and in vehicle tyres. Griffiths, Hugh and Jenks (2012)[v] provide an overview of how criminal organisations use maritime transport to smuggle a range of items and also undocumented migrants, and making use of containers to do so, and also identifying the types of vessel and flag states most likely to be involved in smuggling activities.

Land-side security measures

Ports falling under the ISPS code are required to put measures in place to ensure the security of the port area. This includes both land-side and water-side security (including underwater security). The main land-side issues are: perimeter security; securing connections to utilities (electricity, gas, water supply, telephone or digital networks); protection of infrastructure including equipment, secure storage areas, bonded warehouses, offices and other staff accommodations; any areas where hazardous materials including chemicals are stored; and detection measures to identify smuggled items. In respect of perimeter security, a combination of stationary and mobile patrols, including canine patrols, can be used to monitor the perimeter area in addition to secure fencing, CCTV cameras, motion detectors and other technological systems to detect intruders.

Entrance and exit gates should be manned at all times and, depending on the nature and size of the port, separate gates may be necessary for pedestrians, vehicles, and for truck/rail container transport. In addition, systems to monitor for drugs or explosives should be considered at access points, including canine sniffer dogs, to ensure such materials do not get into the port. This can include vehicle and cargo inspections outside the secure port perimeter.

A system of identification badges, with different colours for different groups of workers or individuals, together with monitoring who is in the port at any given time is important, as is ensuring that anyone who leaves the employ of the port returns his/her badge. CCTV should also be used to monitor individual movements around the port and control access through security doors. Biometric systems such as retinal or fingerprint scanning may also be used in conjunction with keypad entry systems in areas containing high value or high risk materials, over and above standard security measures. Night time security of those areas can be improved with the use of infra-red and pressure-sensor systems which are triggered by any movement in, for example, bonded warehouses or buildings containing electrical and telecommunications systems.

Water-side and underwater security measures

Protecting ships from attacks by surface vessels is one of the water-side security threats facing some ports, particularly those where military vessels berth during a voyage. There are also issues with smugglers attaching containers to the hulls of ships entering a port, to be accessed and removed at a later date; divers entering the port directly from the water or by climbing on board a ship; or submersibles and remote-operated vehicles being used to transport drugs or explosives. Additionally, undocumented migrants may stow away on board ships or in containers. As a result a combination of sea-facing/land-based and underwater security measures are necessary in ports. Sea-facing measures include the use of CCTV cameras (including infra-red) and adequate lighting to monitor for unauthorised people leaving a ship, in conjunction with physical security patrols and canine patrol teams. As noted previously, at night when there should be no movement in an area, the use of motion detectors or buried sensors and cables may also be considered.

In terms of underwater security measures, one of the simplest solutions is the use of underwater lights, fixed cameras and video systems, or remote operated roving cameras, to monitor the area for incursions. Diver interdiction systems, using low frequency acoustic energy can be used to deter divers from approaching a port or ships from below the surface and are particularly useful in high threat areas such as around military vessels or high value targets. In addition, passive acoustic monitoring using hydrophones (underwater microphones) can be used to listen for underwater sounds that may be caused by a submersible, where the noise generated by its motors will be different from that generated by surface vessels. Such a system would be particularly useful in a port where there is limited or no night-time movement of ships. Also in those ports, a system of underwater security nets may be useful in preventing intruders from accessing the port both above and below the waterline. Different types of physical barriers are available and include suspended nets containing fibre optic cable which identify where the net is cut, with sections that can be raised and lowered to allow ships to enter or leave the port, while floating barriers also exist which can be used to prevent incursions by fast boats. The choice of whether to use underwater cameras, diver interdiction systems or some form of physical barrier will, of course, depend on the type of security threat facing a port, and the cost of the different systems.

About the author

Dr Angela Carpenter has been involved in research into how international and European Union policies impact on the activities of maritime ports and installations and on marine environmental protection. She has been conducting research for nearly 15 years and obtained her PhD in 2005. Recently she has been working on issues around security of maritime ports and harbours, and ship security.

Enquiries

Tel: +44 (0) 7531248610
Email: a.carpenter@leeds.ac.uk

References

[i]International Maritime Organization (undated). ISPS Code - FAQs and links to further information. Available at URL: http://www.imo.org/blast/mainframe.asp?topic_id=897#what

[ii]International Maritime Organization (2013). International Convention for the Safety of Life at Sea (SOLAS) 1974. Available at URL: http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

[iii]International Maritime Organization and International Labour Organization (2003). Code of Practice on Security in Ports. Available at URL: http://www.imo.org/OurWork/Security/Instruments/Documents/ILOIMOCodeOfPracticeEnglish.pdf

[iv]United States Customs and Border Protection. Container Security Initiative 2006-2011 Strategic Plan. Available at URL: http://epic.org/privacy/surveillance/spotlight/1006/csiplan.pdf

[v]Griffiths, Hugh and Jenks, Michael (2012). Maritime Transport and Destabilizing Commodity Flows. SIPRI Policy Paper 32 of January 2012. Pub: Stockholm International Peace Research Institute, Stockholm. Available at URL: http://books.sipri.org/files/PP/SIPRIPP32.pdf