Threats from below

A number of incidents in recent years confirm that the threat to international security, infrastructure and commerce has spread to the maritime sector

William Grant, Port Technology International, London, UK

Attacks on shipping in and around ports, such as those on US Navy destroyer USS *Cole* in the port of Aden, 12 October 2000, and on French oil tanker the *Limburg* as it was approaching the Minah Al-Dabah oil terminal in the Gulf of Aden, 6 October 2002, demonstrate new tactics being used to breach harbour security.

The 2004 suicide speedboat attacks on tankers moored to the Bakr oil terminal outside Iraq's Basra port highlight the possible consequences to the world economy if such an installation was attacked. And in March 2005, the Associated Press reported the Philippine military had confirmed that terrorists are being trained to use scuba-diving equipment to attach explosives to a vessel's hull.

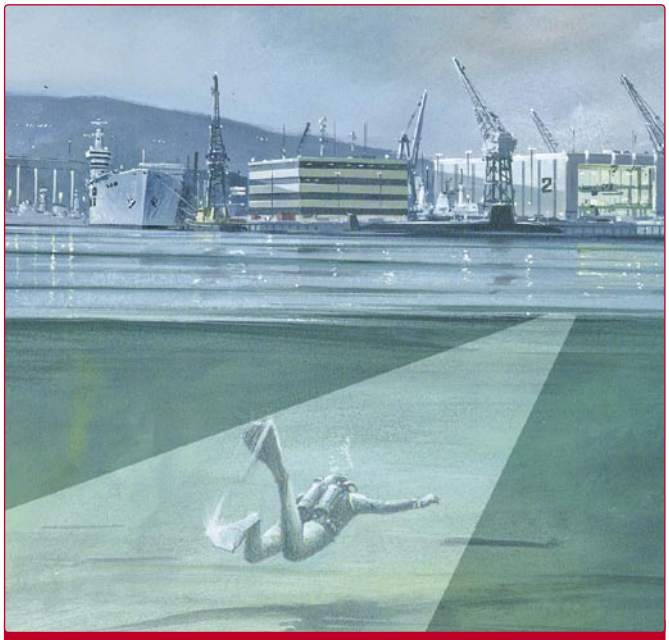
Those investigating the *Limburg* attack were told that Al-Qaeda had at one stage considered using divers and had trained personnel for this type of underwater attack. In the end, a suicide boat crew was used, but it alerted the maritime community to the threat posed by divers attempting to infiltrate coastal facilities or attach limpet mines to ships in port. The threat has already been demonstrated in Sri Lanka where 'Tamil Tiger' (Liberation Tigers of Tamil Eelam) separatists have successfully used divers to attack and sink ships in harbour.

The ISPS code

In 2004, International Ship and Port Facilities Security (ISPS) Code was established to create a framework for governments, agencies and the shipping industry to co-operate to ensure the security of ports and vessels. Since 95 per cent of world trade is transported by water, this is of crucial importance to all trading countries.

Within the maritime industry, ports are seen as key targets. Ships carrying hazardous substances such as liquefied natural gas are also at risk. Potential forms of attack range from: improvised explosive devices being attached to port structures or vessels berthed in and around ports; acoustic mines delivered to the seabed within a port; small-boat attack; hijacked vessel collision; and dirty bombs carried within cargo containers, either for detonation at the port or for later use further inland.

The Achille Lauro incident in 1985 brought basic maritime security issues to light.



Those investigating the 2002 attack on French-registered tanker Limburg were told that Al-Qaeda had at one stage considered using divers and had trained personnel for this type of underwater attack. In the end a suicide boat crew was used, but the maritime community has woken up to the threat posed by divers attempting to infiltrate coastal facilities or attach limpet mines to ships in port.

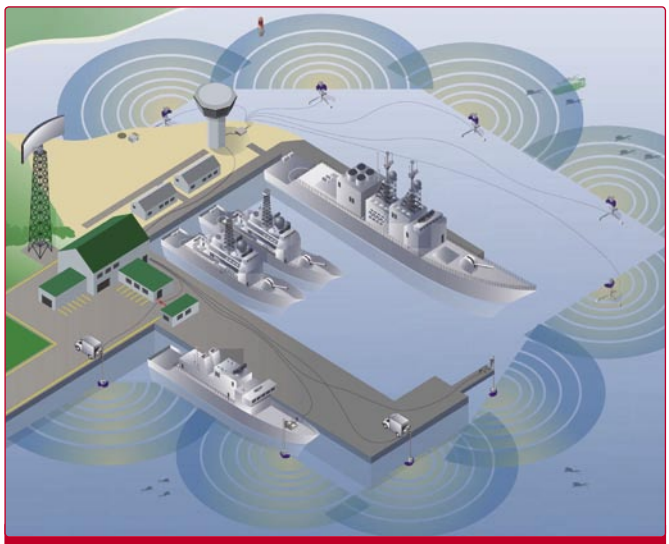
The ISPS Code requires port authorities to maintain effective security within their facilities, enabling them to ensure secure perimeters and control staff, passengers and cargo moving through their gates. Much of the technology required to do this already exists in the form of surveillance equipment such as CCTV and electro-optic sensors and sonar linked to monitoring centres. These are backed by physical patrols of the perimeter, container/vehicle scanning, passenger profiling and staff control.

Waterside security requires above- and below-water detection and sophisticated imaging systems. Commercial ports have been using vessel traffic systems (VTS) for some time and these have evolved to incorporate enhanced features that are suited to the detection of suspicious and unauthorised traffic behaviours.

Technology developments

The threat of terrorist attacks on naval bases, harbours, ports, oil platforms, terminals, underwater pipelines, shipping and coastal facilities is a real and growing concern to all countries and one which could severely affect their economic stability, cause the catastrophic loss of life and damage to infrastructure.

It is acknowledged that terrorist organisations are training operatives in diving techniques and the risk of attack on facilities from diver teams is very real. The need for an integrated marine defence programme has never been greater.



Many diver detection sonar on the market can be used as a single unit to provide area protection or in greater numbers to form a security perimeter, with each unit acting as a node in a wider network.

Undesired 'visitors' tend to approach submerged from sea – swimmer intruders in particular pose a major threat. This line of attack is difficult and expensive to survey and to protect. A wide range of defence solutions can be deployed to detect and respond to such threats.

In response to this emerging threat, and reflecting the heightened port security posture demanded by it, the use of sonar technology to provide early alert of a submerged threat has received much attention from industry.

Diver detection sonars (DDS) are designed to counter the threat of sabotage and terrorism for naval bases, commercial ports and other maritime infrastructure such as oil platforms, underwater cables and pipelines. They automatically detect intruders and provide early warning, a prerequisite for an effective counter-measure.

A number of firms also specialise in VTS systems, such as Belgium-based Barco or the UK's Transas, which supplies ISPS-compliant integrated systems suitable for small- and medium-sized ports.

EADS has bolstered its maritime security portfolio with the joint acquisition – with Germany's ThyssenKrupp Technologies – of Bremen-based Atlas Elektronik. Atlas' Maritime Systems business unit offers a number of above- and below-water systems for port and harbour security and has a specific ISPS offering known as the Seaport Threat Assessment and Response System (STARS).

Kongsberg Norcontrol IT also has significant experience in this area, with products such as the VTMIS 5060 vessel traffic management and information system. This can monitor vessels as they approach their berths and give alerts and warnings of potential incidents including loss of contact, danger of collision and possible incursion into restricted areas, all relevant to the day-to-day running of the port but also to identifying potential terrorist activity.

Thales, an international expert in mission critical systems, has a homeland security solution known as SHIELD, drawing on its security and safety products across the land, sea and air spectrum. The ports of Nantes and Calais are equipped with Thales systems, including visible-light and infrared (IR) cameras as well as supervision software to monitor all port zones.

In late 2006, QinetiQ sold its Cerberus swimmer detection sonar for installation aboard a privately owned super-yacht, which is due to enter service in late 2007. It has also recently leased two Cerberus systems to Spanish contractor Elecnor as part of a comprehensive security system installed in the Spanish port of Valencia for an America's Cup yacht racing ranking event. The two Cerberus sonars were sited to provide coverage of both the inner and outer harbours.

Cerberus is a high-resolution wideband active search sonar capable of detection, classification, tracking and warning of submerged swimmer threats at extended ranges.

In mid-2006, Canada-based Kongsberg Mesotech announced the completion of a DDS installation at a "a high-value seaside resort" in the United Arab Emirates (UAE). The system is based on Kongsberg's SM2000 sonar as the main survey and detection device, linked into a Defender target-plotting processor for a shore-based operator and an Enforcer underwater acoustic defence system from the UK's Westminster International.

According to Kongsberg, trials at the UAE site successfully demonstrated the ability to force intruding divers to the surface at ranges out beyond 1,000m.

In late 2007/early 2008 Israeli's dsIT Solutions Ltd will deliver its Diver Detection Sonar (DDS) to oil terminal operator Naftoport to guard the facility in Gdansk, Poland, against diver incursions. The purchase is thought to be the first commercial sale of a diver detection device to protect a critical coastal energy installation.

Naftoport operates the Gdansk oil terminal, playing a key role in transporting crude oil to Polish and German refineries and in exporting Russian crude oil worldwide. The DDS will form part of a larger integrated above-water and underwater security system. It comprises a PC-based command-and-control computer connected by a fibre-optic link to a number of sonar nodes positioned on the seabed or attached to a pierhead.

ABOUT THE AUTHOR

William Grant is a freelance maritime defence journalist with over 10 years experience in the industry. Publications he has written for include Jane's Navy International, EEZ International, International Ship Operator and Port Technology International, among others.

ENQUIRIES

Angus Dawson
Editorial Manager
Port Technology International

Email: adawson@porttechnology.org
Website: www.porttechnology.org