The Institution of Engineering and Technology

Global challenges in maritime security

Although piracy attacks off Somalia may be abating, there is no decline in sea terrorism worldwide. On the contrary, our sea trade routes may never have been more vulnerable and threat to economies through disruption of maritime lines of supply never more relevant.

> “Piracy can only be addressed by means of a comprehensive multi-layered approach that involves political, technology and societal measures, to strengthen security capabilities, improve intelligence gathering and sharing, and help bring about more effective law enforcement. It also requires multinational cooperation on land and at sea.”

Transport

✈ 🚕🚌 🚢 🚆

Over 50,000 merchant ships ply the seven seas. ISO container traffic is more or less back to previous levels. There are more than 200 million container movements involving the USA alone. And world sea trade is expected to increase significantly over the next few years.

Cruising on the high seas is booming. The industry is responding by building bigger and bigger ships. The latest Caribbean cruise ships, the OASIS class, weigh in at 225,000 gross tons and carry 5,400 personnel onboard.

There has been much publicity surrounding the use of armed guards at sea; but much less on how engineering and technology can play its part in reducing the sea terrorism threat.

In co-operation with the Security Association for the Maritime Industry (SAMI), this Transport Sector Insight examines the security threats at sea and considers the technologies that are available to help reduce this threat.

www.**theiet**.org/transport

The Challenge

Governments know that sea terrorism will only be contained when our seas are policed effectively. The need to have a structure that addresses maritime security capacity building and involves both regional and extra-regional countries is understood if not yet practised.

Such improvement requires leadership and inspiration from the United Nations. Until then, governments, maritime institutions and the maritime industry at large can all make (preferably cohesive) initiatives and contributions to containing the maritime security threat.

Sea Piracy

Piracy affects much less than 1% of 23,000 ships that pass through the Gulf of Aden and even less in the Indian Ocean. But the real cost of piracy is reflected in the need for fleet owners to pass on the extra fuel measured in tons per day required to divert around terrorist / piracy areas.

Frontline Ltd. the world's largest supertanker fleet, estimates that the diversion costs for one of their ships is in the region at about $100,000. There is also the fuel used to sail faster to avoid pirates boarding in the danger zones. Shippers must pay higher insurance premiums, harden ships (just the barbed wire for one ship can cost $10,000), hire security crews, and provide training and equipment. There are some rule of thumb costs, but each voyage has unique expenses related to piracy. All of these costs must be folded into what they charge for their transport and the cargo owners will add the cost of the increased shipping into their products to the consumer. This may be small and barely noticeable in terms of cost per unit item on the supermarket shelf but significant when taken together.

Elsewhere, terrorism at sea has emerged with even greater consequences. According to the International Maritime Bureau's Piracy reporting centre (IMB-PC), there have been at least 40 piracy attacks on vessels in the Gulf of Guinea this year and that, in 19 cases, vessels were boarded and eight successfully highjacked. Piracy continues around the western edges of the Pacific Rim, in the Caribbean and, worryingly, recently off the coast of Brazil, close to some of its offshore installations.

Back in 2010, Rear Admiral Bernhard Teuteberg, Chief Director Maritime Strategy for the South African Navy reported, "The importance of transport in supporting socio-economic development and African regional integration cannot be over-emphasised. In that context, maritime transport remains the most feasible means for facilitating trade between continents and islands. Its role is particularly enhanced in Africa whose exports are made of largely primary unprocessed commodities i.e. bulky agricultural and natural produce. About 90% of the total trade of Africa is seaborne".

In the waters off Nigeria, hijacking of cargo and commodities has increased by over 140% in the last 18 months, often accompanied by aggressive action by pirates / terrorists. People have been killed.

www.theiet.org/transport

How can technology play its part?

The Cruise industry sees reasons for investing in technology, albeit for the benefit of passengers' comfort. Modern cruise shipping companies are IT savvy. In response to customer expectations, Carnival Cruise Line OASIS class are equipped with 900+ wireless access points, 30,000+ IP ports and 1,200 wireless phones linked by 600,000 metres of fibre cable and 44 network switching locations.

They are also equipped with state of the art photo recognition software linked to high resolution webcams to take photographs of guests as they arrive onboard. In other passenger vessels, there are cyber security controls and great efforts are taken to manage bandwidth, the scourge of sea going vessels, utilising packet software optimisation for example and ensuring that email traffic between passengers onboard stays within the vessel.

In smaller vessels, companies such as Selex UK have introduced Oceanlink; a Very Small Aperture Terminal (VSAT) which brings together, at an affordable cost, broadband internet and VOIP connectivity for vessel operators. Some logistics companies have seen the light by investing in stopping crime before it happens rather than solving crime after the event, but this pragmatism is not reflected across the maritime industry at large.

Yet despite the fact that Oceans Beyond Piracy – a respected US based Think Tank reports that Somalian piracy costs the world economy at least US$7 billion and other institutions believe that world sea terrorism is affecting world economies to the tune of at least US$25 billion, the shipping sector remains remarkably unprepared.

In piracy infested waters, shipping owners have resorted to the use of armed guards, often with success, but with significant cost, and technology measures often boil down to use of razor wire, some enhancements to physical protection and occasionally the provision of safe areas or Citadels. There is little investment in long term solutions that detect, track, identify, respond and record to prevent a terriorist act before it occurs and to optimise deterrence and avoidance. Nor has there been much enthusiasm for ship redesign to provide long lasting security capability or a detailed investigation by many shipping companies into what proven technologies exist and how they can best be system-integrated and supported in relation to the threats and the risks.

At the recent SMM Security & Defence conference 2012 in Hamburg, the Group Security Officer for Hamburg Sud gave a straightforward, factual and pragmatic presentation on the technologies and training that Hamburg Sud has embraced to reduce the terrorist / piracy threat in their vessels and prevent crime where it is relevant. Hamburg Sud has taken a long term view, has an incremental capability policy and places great emphasis on so called collective training. That is training

www.theiet.org/transport

all personnel together (simulation, real time practices and after action events) to deal with unforeseen situations, potential crime issues and piracy deterrence and avoidance. Hamburg Sud is a rare exception.

What needs to be done to foster technology approaches?

This Sector Insight only scratches the surface. Systems integration, risk management and information management / data fusion are core elements of any technology solution once a requirement has been verified. A number of Consortia has formed around these three core elements assisted by SAMI expertise to penetrate the maritime security market: reduce the risk to cargo and people at sea, reduce insurance premiums and improve the resilience of sea supply chains. Core capabilities are enhanced on a case by case basis by:

- defensive aids which includes light intensity and sound intensity devices
- physical protection which includes the installation of safe havens or so called 'Citadels'
- underwater detection
- above water detection
- advanced intelligence capabilities, which include the ability to verify track formations of surrounding vessels, verify whether they are friend or foe and then recommend or take countermeasures.

One example of a new integrated technology has been developed by Watchstander©, a progressive company based in the USA. WatchStander is built on the premise that pirate behaviours are purposeful and distinguishable from most other behaviours in the at-sea environment.

As it stands at the moment, WatchStander uses off-the-shelf systems commonly available (thereby keeping costs pretty low) and the heart of the system is the computer algorithms developed by Penn State University with a US Navy contract. Hardware consists of a sensor suite comprising a detection sensor (the SIMRAD 4 4G) continuous wave frequency modulated radar which passes data on all targets detected to the WatchStander software and a location / movement sensor comprising an MTI-G inertial measurement / GPS unit which passes movement and location data of own platform to the WatchStander core software.

The countermeasures unit is mounted on a FLIR D-100 pan and tilt unit and consists of a peakbeam 12 million candlepower light, capable of both fixed beam and strobe lighting and laser, video camera and laptop computer, with large external monitor.

The system uses WatchStander's proprietary software which forms tracks, evaluates tracks and operates countermeasures. The combined capability can:

- accept radar targets and builds tracks of target movement over time
- examine tracks for pirate behaviour
- when pirate behaviour is found, direct a tailored countermeasure suite engagement of the pirate
- determine priority of targets and shifts countermeasure system to highest priority
- select appropriate countermeasure for range and priority
- provide alarm data to ship crew
- provide prioritised targeting data to security team

The SIMRAD radar is high-definition (high frequency) continuous wave, with a data refresh rate of 1.67 seconds. The radar picture occupies two-thirds of the screen, with a one-third column on the left demonstrating target data and analysis. Once the software is switched in, it analyses the screen data. Items which are fixed (land, buoys, navigation markers) are displayed for reference. Targets above a configurable speed are classified and ignored. Targets below a configurable speed (say, stopped) are ignored. All other targets are analysed, and given target circles (known as error eclipses) around them and a target number. The larger the error ellipse, the vaguer the system is about the target. The ones that are of interest have very tight error eclipses, not much larger than the contact paint on the screen.

The algorithms check the targets for behaviour that could be construed as piratical, either in shadow mode (i.e. matching course and speed with the home vessel) or aggressive, in that it looks as if an approach is being made to the home vessel. The system also looks for "hiving", when a target vessel suddenly develops additional tracks, as in a mother ship dropping small craft for attack. For each target, CPA and time of CPA are calculated, and are critical factors in helping the algorithms prioritise targets.

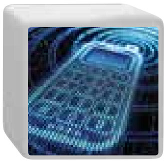
The system is set to start alerting at a given distance. The output is also stored on hard disk for later review and analysis. If multiple 'hostile' targets are detected, the system determines the most immediate danger, and concentrates on that. It will switch to a different target if that becomes potentially more dangerous.

Other technical developments

This Sector Insight can only touch on examples of the technologies being developed or introduced.

Watchstander© is just one of the capabilities being offered into the maritime security market to provide better protection to crews and passengers and is an excellent example of entrepreneurship between private, research & development and military, coming together for common good.

Other organisations also provide advanced risk modeling and toolsets, often proven in adjacent sectors such as insurance and business continuity sectors, and companies providing communications bearer services or data service that allows transmission of information signals between network interfaces.



www.theiet.org/transport

Traditionally, communication transmission at sea has involved an unwieldy mix of providers (Inmarsat, Iridium) and services, but some companies now provide single shipboard computer interface for managing email and data services, which significantly reduces the cost of data transmission.

A lot of effort and investment is going into intelligence gathering using a combination of data mining and fusion which is then allied to decision making in which the human operator is very much central to the decision making progress. Global Intelligence gathering also uses predictive behavioural software and the ability to pick out key information from millions of bits of background data.

The Future

- It is a long haul to introduce technology based solutions.
- The maritime industry is fragmented and not especially transparent.
- Nations need to facilitate vibrant maritime commerce and economic activities at sea and these requirements underpin economic security.
- At the same time governments strive to protect their maritime domains against ocean-related threats such as piracy, criminal activities, terrorism, pollution, etc.

These objectives require a commitment to develop effective technology-based solutions drawing on public, military and private sector capabilities to counter this increasingly dangerous maritime threat to the world-wide economy.

To be effective in making the global shipping business safer and cheaper, inside territorial waters of independent nations and in the open sea, cooperation is essential. Collaboration on technical solutions requires new approaches to contracting mechanisms and protection of Intellectual Property.

However, there are many in the maritime industries who consider that threat reduction is at a tipping point. Whilst there will always be a market for guard forces, many governments are beginning to see the benefit of investing in maritime technology. The insurance industry has a significant role to play here in advocating lower risk (to human life) technical solutions that reduce costs to the industry.

About this Insight

This Sector Insight has been written in collaboration with SAMI, a not-for-profit trade association which lobbies on behalf of its members to improve maritime security globally.

Barry Brooks, Deputy President IET says:

> “Whilst the public only hear about piracy and maritime terrorism when there is a serious incident, the problem is continuous and the costs to the industry, and hence to the end consumers of maritime trade, are growing. As in other armed conflicts, technology could provide more reliable, effective deterrents and safer counters. Meeting that challenge is what IET’s engineers and technologists can do. Through Insights like this, and by enabling debate, the IET’s Marine Transport Group encourages innovation in the search for effective solutions.”

You can get involved by contributing your views on the Transport Sector community at

www.theiet.org/transport-community