the BRIDGE

November 2016

REDUCED HRA HAS A FINANCIAL IMPACT ON PMSCS

CYBER SECURITY CHALLENGES IN THE GULF OF GUINEA

OUT OF AFRICA: MTISC TO MDAT

PROLIFERATION OF CONTRACTED MARITIME SECURITY SERVICES

SECURITY CONSIDERATIONS FOR UNDERSEA MINING

AN OBJECTIVE REVIEW OF THE CSO ALLIANCE

Welcome back to theBRIDGE

theBRIDGE returns full of energy and enthusiasm and will be published quarterly and sent out to our readership free of charge. We hope theBRIDGE will prompt debate and discussion, as almost all of the subjects we will examine will be constantly evolving. We want to engage with our readers and are very keen to hear your thoughts and opinions, some of which we will publish in the next issue of the BRIDGE. If you want to make a comment or initiate a debate please write to bridge@pcamaritime.com

The reinvigorated magazine is independent and self-determining, able to examine new subjects and global events carefully and objectively, provide balanced analysis and look at how security concerns may affect the maritime industry. But what, some of you ask, is maritime security? What does it mean, what does it include? How does it affect me? This is one of those very challenging questions, as it can mean very different things to different people depending upon whether you are an Admiral, a commercial ship owner, a fisherman, the superintendent of an offshore platform, a harbour master or a member of a community living on a coastline.

Here's an overview of what's inside this issue...

theBRIDGE is published by PCA Maritime

Executive Editors - Peter Cook & Chris Ashcroft

Editorial Contributors - Stephen Askins - Tatham Macinnes, Peter Cook - PCA Maritime, Sean Duncan - Oceans Beyond Piracy, Stephen Spark, Sandra Speares, Templar Executives, Phillip Taylor MBE

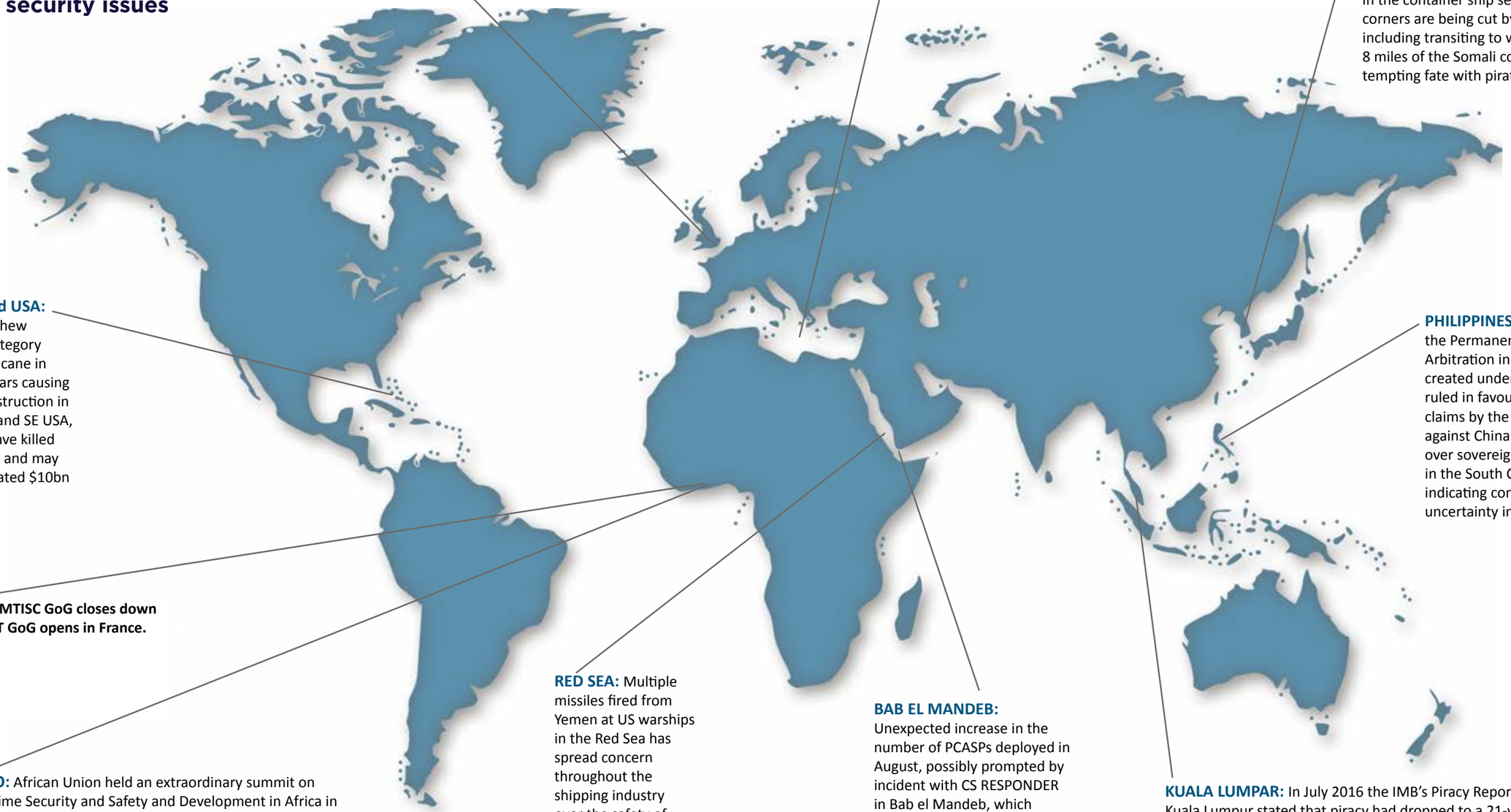
Production - Seren Creative

Advertising - Portcare International www.portcare.com | info@portcare.com

theBRIDGE - November 2016

Global Maritime Security Roundup

Independent global maritime security consultants PCA Maritime provide an overview of current international maritime security issues



UNITED KINGDOM: The UK Government's Department for Transport (DfT) have worked with the Institute of Engineering and Technology (IET) and other agencies to publish a set of guidelines entitled Cyber Security for Ports and Port Systems.

MEDITERRANEAN SEA: The death toll of migrants crossing the Mediterranean by sea has reached 3,654 (20 Oct 16) the Missing Migrant Project reported. It is likely that 2016 will see the highest number of migrants dying at sea.

REPUBLIC OF KOREA: Container shipping company Hanjin declared bankrupt. Symptomatic of overcapacity in the container ship sector, corners are being cut by some including transiting to within 8 miles of the Somali coast tempting fate with pirates.

Caribbean and USA: Hurricane Matthew was the first Category 5 Atlantic hurricane in more than 8 years causing widespread destruction in the Caribbean and SE USA, estimated to have killed more than 550 and may cause an estimated $10bn of damage.

PHILIPPINES: In July 2016 the Permanent Court of Arbitration in the Hague, created under UNCLOS, ruled in favour of seven claims by the Philippines against China in claims over sovereignty of islands in the South China Sea indicating continued uncertainty in the region.

GHANA: MTISC GoG closes down and MDAT GoG opens in France.

TOGO: African Union held an extraordinary summit on Maritime Security and Safety and Development in Africa in Lomé, Togo in mid October designed to establish a "road map" for maritime security and make the maritime space the key driver for sustainable economic development in Africa.

RED SEA: Multiple missiles fired from Yemen at US warships in the Red Sea has spread concern throughout the shipping industry over the safety of commercial ships moving to and from the Suez Canal.

BAB EL MANDEB: Unexpected increase in the number of PCASPs deployed in August, possibly prompted by incident with CS RESPONDER in Bab el Mandeb, which turned out to be a false alarm but demonstrates shipping industry nervousness.

KUALA LUMPAR: In July 2016 the IMB's Piracy Reporting Centre in Kuala Lumpur stated that piracy had dropped to a 21-year low. Two main factors were recent improved cooperation between agencies around Indonesia and continued active deterrence off Somalia.

OBITUARY: SECURITY ASSOCIATION FOR THE MARITIME INDUSTRY

On 10th May 2016 the Security Association for the Maritime Industry (SAMI) was formally placed into voluntary liquidation and the representative body for the private maritime security industry ceased to exist. This obituary is a synopsis of what the Association achieved in its five years in operation and what led to the decision by the Board of Directors to wind-up the organisation.

We often forget, but when SAMI was launched, in May 2011, at the height of piracy off the coast of East Africa, 26 ships were held by pirates (17 of which had been hijacked in the first 5 months of that year) and hundreds of seafarers were detained on board the ships, held for ransom, in horrendous conditions of depravity, routinely subjected to psychological abuse, torture and worse.

But after a number of irresponsible incidents involving private security companies, particularly in Iraq, the shipping industry demanded a robust regulatory structure to ensure professional standards across the emerging private maritime security industry.

SAMI's mission was to provide a list of reputable private maritime security companies (PMSC), allowing ship owners, flag States and marine insurers to make informed decisions about which PMSC to select to protect their crews, cargos and ships transiting the High Risk Area (HRA). Within just over one year of launching, SAMI had 180 member PMSCs from 35 countries around the globe demonstrating, unquestionably, that SAMI was important and necessary. It was also a clear indication that this new industry wanted an international voice, welcomed regulation and sought to demonstrate its professionalism in the provision of security services to the commercial shipping industry, and to protect seafarers in the piracy-infested waters of the North West Indian Ocean.

From inception SAMI was intimately involved in the development of standards for the industry. Initially they actively took part in discussions at the IMO which led to the development of two foundation MSC Circulars (1405 & 1406), which in turn provided the basis for the SAMI Standard developed with SAMI's Standards and Accreditation Working Group (SAWG). At the beginning of 2012 however, it became apparent to SAMI that the international maritime community would not accept self-regulation of the industry. Consequently, the SAMI Standard was submitted, via the Marshall Islands delegation, to the IMO for consideration. The SAMI Standard was a substantial element of ISO 28007 and the CEO was an integral member of the core drafting team.

SAMI also worked hard with the marine insurance brokers Marsh to develop 'the SAMI Facility', a bespoke, comprehensive insurance package designed specifically for the private maritime security industry. This product was awarded the Lloyd's List Business Innovation Award in 2013 and the British Insurance Award for Commercial Lines Broker of the Year in 2013 as well.

In spite of some initial resistance SAMI led the way, with a team of international lawyers, in establishing the 100 Series Rules for the Use of Force (RUF) that would provide the legal structure and substance for PCASP to protect ships against piracy attack, bringing together the International Chamber of Shipping, Marshall Islands Registry and other shipping associations to help develop the rules. This model set of RUF are used extensively today by ships transiting the HRA.

As part of an International EU Consortium, which included the World Maritime University in Malmo and several major maritime industry entities, SAMI was an integral part of the European Commission's 7th Framework Programme for Research, Technological Development and Demonstration. This clearly evidenced SAMI's commitment to maritime security utilising not only armed guards but equipment, technology and hardware to mitigate maritime security risks.

To provide a voice for the private maritime security industry at the strategic level SAMI represented them at a number of international forums including; (as part of the Marshall Islands delegation) the IMO, the International Contact Group for Piracy off the Coast of Somalia (CGPCS), the European Commission's Stakeholders Advisory Group for Maritime Security (SAGMaS), G7++Friends of Gulf of Guinea Group (FOGG). This proved to be fundamental in the way that opinions at the highest level on the use of armed guards were developed and the concept became accepted.

SAMI successfully published eleven editions of a quarterly magazine, providing high quality insight for the maritime industry into the private maritime security industry as it evolved, and explored many aspects not covered by other publications.

The Association also ran a series of 8 events on board HQS Wellington in London, covering topical areas of concern for the maritime industry including the use of citadels on ships transiting the HRA, port security, 100 Series Rules for the Use of Force, Lessons learnt from the implementation of ISO 28007, Maritime Cyber Security and focusing on the very different aspects of maritime security in the Gulf of Guinea.

In a very short time, SAMI established an impressive global presence across the shipping and marine insurance industries and the Association won several industry awards including the Lloyd's List, Newsmaker of the Year award in 2012. The Association's CEO, Peter Cook, was named by Lloyd's List as one of the 100 most influential people in the shipping industry in 2012 and 2013.

SAMI was also invited to speak at a multitude of important conferences and events on countering piracy at sea across the world, providing an unparalleled insight into how this new industry had evolved so competently and commendably.

SAMI was often approached by the international press for comments on maritime security questions, and to provide informed comment on the complicated issues of providing armed security on ships and the advantages of using professional PMSCs.

In May 2012 the MV Smyrni was the last large commercial ship transiting the HRA to be hijacked and the crew held hostage for ransom. The combination of international naval forces, the shipping industries' Best Management Practice (BMP) and the use of PCASPs to protect ships proved to be an effective deterrent against piracy attack. As a consequence of the reduced threat from piracy the use of PCASP very slowly decreased and the private maritime security industry gradually began to consolidate and SAMI's membership declined in parallel. The Association's Board constantly reviewed the situation and managed the budget very carefully to ensure maximum representation at the least practical cost.

In December 2015 after more than three years without a single ship being taken in the Indian Ocean the size of the HRA was significantly reduced. The impact on the SAMI membership was palpable and within the first three months of 2016 the membership reduced by 18%. After considerable market research it was clear that this was a tangible trend. The predicted loss in subscriptions would put SAMI in a financially untenable position and so the Board, after considerable discussions with the Industry Steering Group, made the difficult decision to close down the Association.

As a post script, in July 2015 the UNODC reported to the CGPCS that they had conducted extensive interviews with the 1,000 pirates in detention. Amongst other questions, the pirates were asked what they were most scared of at sea and the overwhelming response was "the navy". This clearly proves that SAMI did its job and that PCASP protected thousands of seafarers from the terror of hijacking by demonstrating high standards of professionalism and only using reasonable levels of force when necessary to deter pirate attacks.

It is impossible to predict what history will say about SAMI and what it achieved but it was undeniably a positive evolutionary process for the private maritime security industry that proved how a combination of navies, seafarers and security guards can work together in an unprecedented way to overcome an intimidating and dangerous threat in order to maintain the movement of free trade.

REDUCED HRA HAS A FINANCIAL IMPACT ON PMSCs

Stephen Askins of Tatham Macinnes looks at the effect last year's reduction in the High Risk Area has had on the private maritime security industry.

The ripples from last year's reduction in the High Risk Area ("HRA") are still being felt in the private maritime security industry. One immediate impact was MSCHOA reporting a marked decrease in the percentage of ships declaring armed guards on board ships transiting the Voluntary Reporting Area ("VRA"). Fewer opportunities for armed teams at rock bottom prices is undoubtedly effecting the profitability of PMSCs who are scrapping for market share. One senses from the type of cases crossing our desks that the maritime security sector is carrying a significant amount of debt and a question arises as to what extent that is an existential threat to the logistical framework that underpins the maritime security sector. Non- or late paying customers filter through the supply network to all areas, including the all-important floating armouries, which provide the platforms for the weapons and men. A default on the underlying charters of these vessels, and the withdrawal of those armouries, would inevitably mean a sharp increase in the PMSCs operational expenses if they were forced back to land based options, which they would want to pass on. This article looks at the tools that are being deployed by creditors in the pursuit of the debts against UK registered companies.

Against a UK company the first line of attack is often a Statutory Demand ("SD"). This allows a creditor owed more than £750 to file a SD seeking the winding up of the PMSC in 21 days if the debt is not paid. It is on its face a powerful tool particularly if the PMSC (as is likely) is the holder of the various Trade Control Licenses allowing the transfer of weapons between third party countries and the floating armouries. However, the SD is not supposed to be used as a debt recovery tool, and a creditor can find itself on the wrong end of a costs order, if they pursue an SD and do not withdraw it when invited for good reason to do so. This is particularly true if the underlying contract between them provides for arbitration as the dispute resolution forum. In any case where there is said to be a genuine dispute (and that may be no more than the amount is "not admitted") then there is a risk that if the SD is not withdrawn then the PMSC debtor will get an injunction forcing them to do so with the creditor paying their costs. A SD must be taken seriously and a party has 18 days from service within which to make a challenge if they are going to do so.

For the wider EU, the other (under used) tool is the European Order for Payment procedure ("EOP"). It is a similar device to the SD, which applies to commercial matters where it is said that there is no dispute and it avoids unnecessary litigation in a foreign Court. The creditor simply fills in a form, which is filed in the courts in their own country, and the EOP is usually issued within 30 days. If there is no statement of opposition then it becomes enforceable in all EU countries (save for Denmark which does not recognise EOPs).

One senses that the private maritime security industry is at a tipping point and it may yet undergo a financial shock. Pursuing poor debtors is a time consuming and potentially expensive exercise but in cases where the client won't pay and there is no dispute there are cost effective ways to get the invoices paid without resorting to arresting assets like the ships on which armed guards have been deployed.

Stephen Askins who left the Royal Marines in 1990, joined Tatham Macinnes in April 2015 after 25 years at Ince & Co.

In recent years he has become recognised as one of the leading experts advising on piracy, maritime terrorism and the use of armed guards. He advises on the legal and practical issues that arise for clients operating in complex environments including Libya, Crimea, the Indian Ocean and the Gulf of Guinea. He has handled many hijackings and kidnappings on both east and west Africa working with owners and their Crisis Management Teams.

He was part of the GUARDCON drafting committee and appeared in front of the Foreign Affairs Committee looking into piracy off Somalia. He was also part of the Industry Advisory Panel working with the International Task Force set up to debate the legality and payment of ransoms.

Please send any comments on this article to **bridge@pcamaritime.com**

A GULF BETWEEN:

CYBER SECURITY CHALLENGES IN THE GULF OF GUINEA

Several miles off the Nigerian coast in the Gulf of Guinea, a container ship is slowly making its way on a parallel course to the shore. All of a sudden a cry goes up that a go-fast is approaching from the stern and making good pace on the vessel. The officer of the watch looks from the bridge and identifies a potential pirate vessel with several heavily armed young men aboard.

Immediately counter-boarding measures are initiated, barbed wire is checked and water cannons are started. However, these basic measures are not enough and the pirate vessel is able to get alongside and the pirates clamber onto the ship. The crew head to the citadel. In a much shorter time than expected, the pirates leave the ship and the go-fast and a heavily laden support vessel make their way towards the shore. When the crew exit the citadel they find that only 2 containers have been opened and emptied.

The ship is the latest victim of cyber-enabled piracy.

Credit: Tashatuvango/Shutterstock.com

In 2015 there were 54 piracy incidents in the Gulf of Guinea[i] and cyber is a growing element of these incidents.

In early 2016 Verizon made headlines when they published the first official report on cyber-enabled piracy methods as part of their Data Breach Digest[ii]. The Verizon report covers in some detail how attackers compromised a shipping content management system and used this to track Bills of Lading to identify cargo of interest. This information was then passed on to the 'operational' pirates who targeted the ship and removed the contents from the relevant containers. Whilst further examples of these types of attacks are sparse (the maritime industry is notoriously poor at sharing cyber attack information), they do seem to be increasing. It is quickly becoming a case of not if you experience a cyber attack, but when.

The section of the Verizon report detailing Maritime Cyber Piracy concludes with the sentence: 'moving forward, the victim worked to adjust its security posture by starting regular vulnerability scans of its web applications and implementing a more formal patch management process'. For those coming from an Information Security or Information Technology background, this advice won't come as a surprise. However, for those who don't deal with IT on a daily basis this may sound like another language, and herein lays the crux of the Cyber problem. Jargon.

The Cyber Security industry loves jargon. It is important that those working in the industry take steps to demystify the subject, and present it in a way that it is not only interesting and engaging but is also jargon free.

Cyber is increasingly being recognised as everyone's problem, not just an IT problem. All members of a company or crew are expected to behave in a way that is 'Cyber safe', but this can be problematic if information explaining what is 'Cyber safe' is almost unintelligible to the Seafarer or shipping company employee. In all business environments, the person most likely to fall victim to a Cyber attack is the one who unwittingly, or accidentally goes to a website carrying viruses[iii] or clicks on a link or attachment in an email that contains malicious software.

Herein lies the challenge of operating in the Gulf of Guinea. Since the dawn of Internet scams, Nigeria has been playing an active, if low-tech, role. The '419 scams', as they were nicknamed, were very common 10 years ago. These scams begin with an often poorly spelt email promising the reader large amounts of money that is stuck in a Nigerian bank account and all that is needed is your bank account details so they can transfer the money to you and avoid tax or some other excuse. The scammer will then suggest some reason why you are required to pay them some money first (to pay the transfer costs or to bribe a corrupt official etc.).

If the victim pays this money, then a similar event will be invented that requires the victim to pay more money and thus the cycle continues.

Now, however, as people become aware of these ploys, and the political and security situation in Nigeria becomes increasingly unstable, scammers have been turning to other ways to make money. Increasingly across Africa, terrorist organisations are enlisting the help of hackers and pirates to help them keep a steady flow of cash coming in. This was a trend that originated in Somalia, but has quickly spread across the continent.

In order to combat this newer and more physical type of Cyber threat, companies increasingly have to turn to technology to fight technology. As recently reported[iv] pirates are using drones to scout potential targets leading to shipping companies and PMSCs having to deploy drone counter measures and 'killer-drones' to target and repel hostile pirate UAVs. With a range of sophisticated attack mechanisms available to the pirates, it is now more important than ever to ensure that all staff and crew in your organisation understand the basic measures they can take to help protect your company.

Training, education and awareness are vital for ship and shore-based staff alike. Only by having a high baseline level understanding of the threat can individuals keep themselves and their companies safe. One vulnerability that is often overlooked is social media. With a continued pressure on operators to provide increased internet access for crews away from home, there is a heightened threat from crew members posting information online that could alert potential attackers to the ship's whereabouts or contents. According to a 2016 report from Oceans Beyond Piracy[v] rates of kidnap for ransom in 2016 have already surpassed that of 2015. At the time their report was published, there was 32 reported kidnap for ransom incidents so far this year. With this in mind, it is vital that all crew members are appropriately trained and educated so they can understand the risk and keep themselves, their ship and their company safe.

Sources:

[i] http://oceansbeyondpiracy.org/reports/sop2015/west-africa
[ii] http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf
[iii] http://www.calyptix.com/top-threats/top-5-cyber-attack-types-in-2016-so-far/
[iv] http://www.bbc.co.uk/news/business-37257236
[v] http://oceansbeyondpiracy.org/sites/default/files/attachments/2016%20GOG%20Trends.pdf

Templar Executives
Timely, Relevant and Valued Delivery

OUT OF AFRICA

MTISC TO MDAT

The town of Brest, on the Atlantic coast of France, has a long association with maritime crime. It was once a notorious haunt of pirates, who harried ships in the English Channel, so there is a certain irony in its choice as the centre for co-ordinating data on Gulf of Guinea piracy.

Maritime Domain Awareness for Trade – Gulf of Guinea (MDAT-GoG) started operations at 08.00 on 20 June 2016. The French Navy runs it, as the northwest coast of Africa comes under NAVAREA II, for which France has responsibility. The UK hosts a back-up operation at Portsmouth.

MDAT is based on the successful model of the voluntary reporting area (VRA) for the western Indian Ocean, which has been administered by UK Maritime Trade Operations (UKMTO) since 2001. While the UKMTO office is in Dubai, the Maritime Trade Information Centre (MTIC) in Portsmouth provides its 24-hour watch keeping service.

Like UKMTO, MDAT offers a "see and avoid service in response to piracy attacks on shipping", as the UK Maritime & Coastguard Agency (MCA) describes it in recent guidance. All commercial vessels sailing in West African waters are encouraged to register with MDAT and file an initial report when they enter the VRA, with subsequent daily updates at 12.00 UTC and a final report on arriving at a port within the area or on leaving the VRA.

Any unusual or suspicious activity – such as ships not bearing lights, identifiable flag, or name, not using AIS while navigating, sailing outside normal routes or making suspicious approaches should also be reported. Within minutes of MDAT-GoG receiving information about an attack or a threat, a NAVAREA II warning is issued and local centres are alerted.

The MCA notes that the reporting system supports the aims of the Yaoundé Code of Conduct, but it stresses: "MDAT-GoG is a mechanism rather than a new centre – it is a phone and email address that goes to an existing French Marine Nationale maritime information centre… It learns the lessons of the MTISC pilot that came before it, but it is not a continuation of that centre."

MTISC-GoG (Maritime Trade Information Sharing Centre – Gulf of Guinea) opened in April 2014 and closed as Brest took over. Like MDAT, it followed the UKMTO model of voluntary reporting and information sharing. However, it differed from its successor in two important respects: the Oil Companies International Marine Forum (OCIMF) largely funded it and it was based in the region at the Regional Maritime University at Tema, Ghana.

By the time of closure MTISC was receiving 8,000 reports a month. A notable success was the part it played in tracking a notorious 'fishing pirate' vessel, Thunder, which marine conservation group Sea Shepherd pursued on a 10,000-mile chase from the Antarctic Ocean. As Thunder entered Ghanaian waters,

MTISC liaised with the Regional Centre for Maritime Security (CRESMAC) at Pointe Noire, Republic of Congo. Unable to escape this transnational surveillance, the crew scuttled the ship off São Tomé on 6 April 2015. The Chilean captain and two Spanish officers were jailed. Interpol estimated that the Spanish owners had earned up to $60 million from Thunder's illegal fishing activities, demonstrating the pressing economic need for improving maritime domain awareness off Africa.

The generally positive record was marred shortly before closure when BIMCO warned that data security at the centre might have been compromised. Morten Glamsø, senior adviser at the Danish Shipowners Association (DSA), explained: "The Danish authorities at the beginning of the year sent out a warning about a security breach at MTISC and raised some concerns."

The centre denied any security breach, saying it did "not handle commercial or voyage sensitive information". However, some sources suggested that the warning made some ship operators nervous about sending in reports. Coincidentally or otherwise, in early July MDAT alerted vessels to attempts by unknown actors to acquire potentially sensitive commercial information from vessels by an apparent 'phishing' scam.

MTISC was a pilot scheme and never intended to be a long-term fix. Several G7++ countries supported it, and watch keepers were drawn from private companies and the navies of Congo, Ghana, Nigeria, Sierra Leone and Togo. However, according to IMO special adviser Chris Trelawny, the biggest challenge was MTISC's lack of formal legal status in Ghana.

He explained: "Everything had to be done on a month-by-month basis, which made it difficult for IMO to support it financially, although it was supporting the centre with contributions from member states. However, it proved its point and lessons have been learned about developing capacity in the region."

So how has MDAT performed and how does it compare with its predecessor? Glamsø told theBRIDGE: "We find it is a really good initiative tackling some of the lack of monitoring in the Gulf of Guinea. To the best of my knowledge all members of the DSA are reporting to the centre." He continued: "It's still very new, so we don't have much experience about it, but we have confidence."

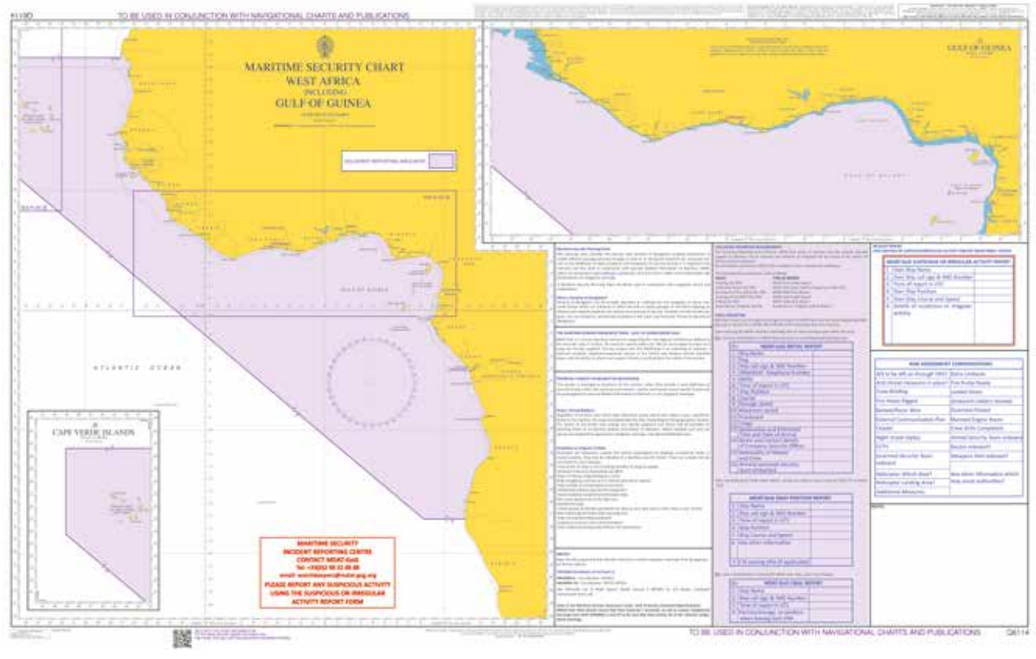
Dan Fearon, director maritime West Africa at Salama Fikira, sees some scope for improvement: "The MDAT-GoG is indeed a very useful tool for information, but the dissemination of its alerts could be improved." In particular, "the online presence of the centre remains very limited [and] MDAT reports could be sent to a larger distribution list".

The decision to set up MDAT out of the region under French and British control was not universally welcomed. "Technically, basing the MDAT-GoG outside of the Gulf of Guinea has likely contributed in solving the issues experienced by the MTISC-GoG; however, from a 'hearts and minds' perspective, the move is counter-productive," Fearon said. "As a short-term solution this was the most immediately effective way to solve the issues experienced by the MTISC. However, the long-term solutions to combat piracy in the Gulf of Guinea will need to be locally driven."

Fearon would like to see regional states set up a joint maritime security agency that would incorporate a maritime intelligence centre to act as a focal point for the collection, analysis and dissemination of piracy-related incidents in the region.

IMO's Trelawny agrees: "MDAT is OK as far as it goes, but IMO was looking at this long-term as developing capacity within the region for combating drugs smuggling, illegal fishing etc. Our intention is to go back to the regional countries and look at opening up somewhere else in the region."

UKHO - Maritime Security Chart West Africa including Gulf of Guinea



Copies can be ordered at: https://www.admiralty.co.uk/maritime-safety-information/security-related-information-to-mariners

THE PROLIFERATION OF CONTRACTED MARITIME SECURITY SERVICES

By Sean Duncan, Oceans Beyond Piracy

Over the last decade, the shipping industry has increasingly turned to embarked armed guards as an emergency measure to protect commercial shipping in high risk areas. The most visible, and the most common, type of armed security has traditionally involved contracting private armed teams to embark vessels. However, in recent years there has been a proliferation of other types of contracted armed security in high risk areas on both the east and west coasts of Africa. These other forms of contracted security include embarked government forces, uniformed embarked guards working for public-private partnerships (PPP), escort vessels and secure anchorages to name a few.

However, oversight mechanisms are not yet in place for these security options, which could cause legal and liability challenges for the shipping industry and Flag States. This short article will define some of the more prevalent types of Contracted Maritime Security (CMS) used at sea and briefly describe existing oversight mechanisms.

The privately contracted armed security personnel (PCASP) model, wherein the shipping industry hires an embarked private security force, has undoubtedly become the most prevalent form of CMS. According to Oceans Beyond Piracy estimates, during 2015 roughly 32% of vessels transiting through the High Risk Area in the Western Indian Ocean Region employed the use of PCASP[1]. So far these teams have enjoyed a high level of success, as private security forces have been capable of deterring or denying almost every piracy and armed robbery attack they have faced.

However, the PCASP model is not the only form of CMS. Throughout the world, various forms of CMS have been adapted to the unique sociopolitical and geographical contexts of specific regions. For example, while PCASP are relatively common off of the Horn of Africa, their usage is expressly prohibited in the territorial waters of littoral states in the Gulf of Guinea—as coastal states want to retain their sovereign monopoly on the use of force. Instead, under the coastal state embarked personnel model, armed teams are drawn from a State's armed forces or law enforcement agencies and hired by a shipping company to protect the vessel while it is in that country's waters.

Oceans Beyond Piracy distinguishes between contracted private services—such as privately contracted armed security personnel (PCASP) and floating armories—and contracted governmental services like vessel protection detachments (VPD), state affiliated escorts, and coastal state embarked personnel. A list of prevalent models of CMS services is included below.

Contracted Private Services:

1. PCASP: Embarked private security force personnel hired by the shipping industry. This model is most prevalent in the Indian Ocean High Risk Area.

2. Floating Armories: Vessels contracted to provide logistical support for private maritime security firms by storing weapons, ammunition and equipment offshore for private maritime security companies, providing temporary berthing for security guards and ferrying guns and guards to vessels needing protection. Their arsenal is usually self-protected by the armory's resident guards.

- Floating armories can be wholly private or part of public-private partnerships
- Floating armories can be stationed in a Coastal State's TTW, under its jurisdiction.
- Conversely, floating armories can be stationed outside of TTW, under the flag State's sole jurisdiction.

Contracted Governmental Services:

3. Vessel Protection Detachments (VPD): VPDs are flag State military personnel embarked on a vessel with explicit approval by the flag State. VPDs most commonly match the nationality of the Flag or are procured through a Memorandum of Understanding (e.g. World Food Program Vessels).

4. State Affiliated Escort: Escort by a State military asset or asset operated as part of a Public-Private Partnership (PPP) under contract from the shipping industry. Examples include escort vessels, or contracted protection in Secure Anchorages and other designated Safe Areas.

5. Coastal State Embarked Personnel: Embarked armed personnel originating from the coastal State, based on arrangements between industry and the providing national authorities – not specifically endorsed by the flag State. These arrangements are common in the Gulf of Guinea and off the Horn of Africa.

- Contracted security services could either come under direct arrangement between shipping companies and the coastal State, or regionally-registered private companies could be used as an intermediary under a PPP with the coastal State.

Sources:

[1] "State of Maritime Piracy 2015: Assessing the Human and Economic Cost | Oceans Beyond Piracy." https://goo.gl/pp451q. [2] Ibid [3] "India Lets Italian Marine Go Home as UN Mediates over Fishermen Shooting | World News | The Guardian." https://goo.gl/EI35ro

With so many different forms of CMS currently in existence, it is no surprise that a similarly piecemeal regulatory system has emerged. The CMS industry is governed and guided by a number of different mechanisms including International Maritime Organization (IMO) Guidance on the Use of Privately Contracted Armed Security Personnel onboard Ships in the High Risk Area, flag State laws and guidance on contracted security, the International Standards Organization ISO 20087, the International Code of Conduct for Private Security Service Providers, the Series 100 Rules for the Use of Force, the Montreux Document, BIMCO's GUARDCON standard contract model, and flag State Letters of Non-Objection or similar document. However, almost all of these mechanisms deal solely with the PCASP model of CMS.

While each of the governance frameworks above applies to certain elements of contracted security, no universal, comprehensive, maritime-specific regulation exists with relation to CMS services—and no central reporting agency exists. The sheer number of different guidance mechanisms creates a lack of uniformity that complicates the usage of CMS and produces regulatory gaps with regard to best practices, use of force applications, and accountability mechanisms. Indicative of this is the fact that there is no formal definition for CMS—and the term may have different implied meanings for a variety of stakeholders.

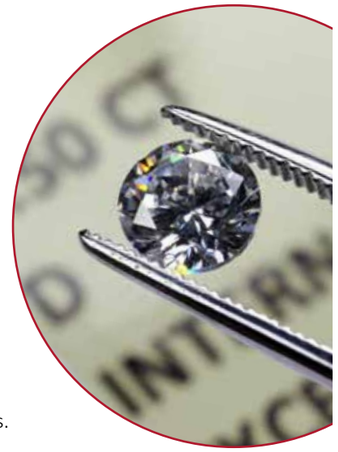
This is concerning as a lack of oversight related to CMS services and the absence of regulation regarding the use of force could place seafarers at unnecessary risk. In the Gulf of Guinea, for example, there have been a number of incidents in recent years in which seafarers have been caught in the crossfire between pirates/robbers and embarked armed guards. In a particularly tragic incident, pirates attacked MT Kalamos on February 3, 2015, boarded the vessel and grabbed two seafarers to use as human shields[2]. Although the Captain pleaded with the armed guards not to shoot, the contracted security team—which was drawn from Nigeria—engaged the pirates and killed one of the crewmembers[3]. No known actions were taken to reprimand the security team.

There have also been many instances of embarked armed guards firing on individuals who were believed to be pirates but were later found out to be innocent civilians, raising serious accountability and human rights concerns. On February 15, 2012, two Indian fishermen were killed off the coast of Kerala, India, because the Italian VPD onboard the MV Enrica Lexie mistook them for pirates. This has led to a number of jurisdictional and legal disputes over CMS services and increased diplomatic tensions between the two states.

To avoid future incidents like these and the negative impacts that may be felt as a result, it is in the best interest of the commercial shipping community to improve the regulatory framework for the use of CMS. Weak and inconsistent regulation, particularly among embarked coastal state agencies, forces seafarers to rely on heavily armed but potentially unqualified guards. A consistent framework would improve safety by shoring up the accreditation and training process—as well as increase transparency and accountability by providing clear guidance for the operation and function of various forms of CMS. Contracted maritime security has proven effective in protecting seafarers in some of the world's most dangerous waters, but providing a comprehensive regulatory system that governs the use of CMS will allow the industry to utilize these necessary services more safely and effectively.

Background Image Credit: Katarzyna Mazurowska/Shutterstock.com
Credit: Andrey Polivanov/Shutterstock.com

With the advent of undersea mining "**Diamonds are Forever!**", but what are the security considerations?



Undersea mining for high value commodities like diamonds is likely to increase in the years to come as on shore supplies become depleted or more costly to access.

While a decade ago most of the diamond mining activity was on land, the emphasis is moving offshore as onshore supplies in, for example, Africa become depleted. Typical operations involve technology to suck sediment off the seabed using a giant hosepipe, after which the sediment is washed on board before passing into a secure area on the ship where a high level of security around the diamond-bearing gravel is maintained. There is no handling by staff and the diamonds are sealed in small containers and escorted ashore by senior crew members to be lodged in a secure location at the home port.

Copper, gold, lead, cobalt, silver and zinc are just a few examples of other minerals in high demand for undersea mining activities. Such activities are regulated by the International Seabed Authority, set up to ensure that such activities do not harm marine environments and comply with the law of the sea convention (UNCLOS). Improvements in the level of technical capability for undersea mining have been key to the development of the business. For example OceanflORE was formed to meet the increasing demand for both expertise and exploitation techniques in the field of deep-sea mining and provides integrated contract mining solutions for offshore mine operators.

OceanflORE incorporates IHC, a Dutch supplier of vessels and equipment for dredging and mining activities, and DEME, a Belgian dredging and environmental services group. IHC is responsible for the development and construction of technical solutions, while DEME handles offshore operations.

Mining companies like De Beers have been making substantial investments in the maritime sector with a view to increasing their production from offshore seams. The first of two new offshore supply vessels to supply De Beers' Namibian operations was launched in Cape Town last year at a cost of $10.5m. The 30 metre tug has a bollard pull of 24.5 tonnes and a shallow draught which enables it to operate out of Port Nolloth, in Northern Cape Province.

A further vessel will be added to support De Beers' mining fleet which operates off the coast of Namibia in the search for diamonds at depths of up to 140 metres. The two support vessels were built at Damen Shipyards in Cape Town and ordered by Smit Amandla Marine which works closely with De Beers.

But De Beers is not the only company to have been investing in ships to support undersea mining, with the announcement of a new vessel being built for its Africa operations, while other operators like Canada's Nautilus Minerals have production support vessels under construction- in Nautilus' case for seafloor operations off the coast of Papua New Guinea.

Nautilus' activities in search of gold, zinc and copper deposits off Papua New Guinea have led to concerns being raised over their effect on fisheries and corals off the coastline. UK Seabed Resources' partnership with Lockheed Martin is another example of offshore mining activity in sensitive sea areas, this time off the coast of Hawaii.

Undersea mining brings its own challenges, not only as far as operating conditions are concerned but in facing up to security issues. With the projected increase in such mining projects, security for these potentially vulnerable ships will clearly be a concern. One recent report on maritime diamond mining suggested employees involved in handling diamonds were not allowed to have dreadlocks to prevent them hiding the jewels in their hair.

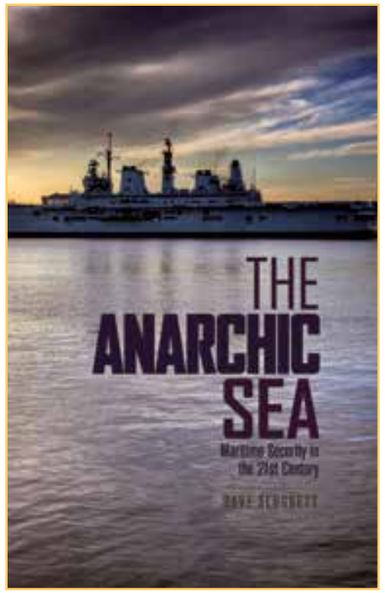
As different extraction companies push to develop offshore mining while shore-based supplies of valuable minerals decline, technology will continue to evolve to allow for operations in more demanding physical conditions at sea. Those countries seeking to take advantage of their undersea resources will need to be certain, however, that mining operations are conducted with minimum harm to the environment. As this sector of the maritime industry grows the safety, security and environmental sensitivity of the operations will be crucial to the reputation and development of this new area.

Editorial: Sandra Speares
Diamond Image Credit: Bjoern Wylezich/Shutterstock.com

Please send any comments on this article to **bridge@pcamaritime.com**

Book Review:

The Anarchic Sea
Maritime Security in the 21st Century
by Dr David Sloggett



Published by C Hurst & Co
ISBN978-1-84904-100-3

Hardback book of 236 pages followed by 2 groups of Case Studies covering 23 coastal States and 10 related thematic subjects, 29 pages of comprehensive notes and 15 page index.

Dr David Sloggett's excellent book was published in 2013 and as the title suggests looks ahead to the way in which maritime security is likely to become increasingly important if not the pivot of security in this century.

Sloggett starts with a very detailed introduction that provides the context of the book, explores the basis of current assumptions about maritime security, and provides a glimpse into how these conventions may be flawed. As you get into the body of the book he proposes his seven dimensions of maritime security from state on state scenarios through maritime crime and terrorism to disasters and oceanography and uses these themes.

Using chapters focused on history he demonstrates why we have established certain norms that shape the way we expect maritime security to be enforced and questions their validity today. He delves in to the importance of the maritime environment, how crucial it is to us, and the criticality of effective stewardship of the seas resources. The threats to maritime security in this unpredictable asymmetric world are examined in detail, and Sloggett explores how our misunderstanding of terrorism may be providing terrorists with extensive freedom of manoeuvre as an unintended consequence of actions on land.

He looks at maritime strategy and how this will inevitably change as the fulcrum of global influence moves from Europe and the Western nations to SE Asia, and the two most populous nations in the world (China and India) increase their dominance globally. He also asks the question about the governance of the oceans, "one of the least governed regions left on the earth." and the effectiveness of UNCLOS.

Looking ahead, Sloggett examines ways in which maritime security may be provided in the coming 80 years, concluding that it is an extremely complex and multifaceted subject that ranges from the borderless effects of cyber security, illegal unreported and unregulated (IUU) fishing and the use of unmanned devices and the adoption of "hybrid naval warfare" by many countries.

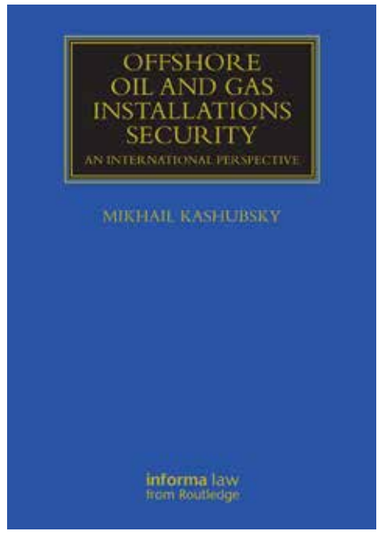
In the annexes Sloggett then examines 23 different national maritime security case studies in detail, providing an excellent selection of scenarios loosely based on the seven dimensions of maritime security in Chapter 1. He then takes this further based on 10 thematic areas from economic migrants, biosecurity, the Mumbai attack, and ballistic missile defence prompting the reader to question how influential these areas of concern will be to different nations. His pages of notes are detailed and extensive, demonstrating the exceptional lengths he went to in research, and the index is excellent.

This book defines a fascinating line for future thinking about the vastness and diversity of maritime security and how it will become progressively more important globally as we move through the 21st century. Whilst we can already see that some of the tactics referred to in the book have been overtaken by events the fundamental principles Sloggett proposes will surely become the reference points as we navigate these challenging waters.

This is an excellent book that provides a detailed historical context and fascinating intellectual thought that provides much food for thought and should prompt fascinating debate; a "must read" for any serious student of maritime security.

Book Review:

Offshore Oil and Gas Installations Security
An International Perspective
by Mikhail Kashubsky



Informa Law from Routledge
ISBN: 978-0-41570-730-5
www.informa.com

Oil and Gas Installations:
A Target for Terror and A Legal Challenge

An appreciation by **Phillip Taylor MBE >** and Elizabeth Taylor of Richmond Green Chambers

We live in an age of terror - and the terror of attacks on the innocent - and also the terror of attacks on specific targets vital to the world economy. Particularly vulnerable worldwide are offshore oil and gas installations – hence the need for this timely legal text from Informa Law: 'Offshore Oil and Gas Installations Security'.

A recent addition to Informa's Marine and Transport Law Library, this is rather a terrific book. Yes, it will be of abiding interest to international and environmental lawyers, but the clarity of the author's prose style will make it accessible, not to mention fascinating, to everybody and anybody interested in this subject which, according to author Mikhail Kashubsky, has hitherto been surprisingly neglected.

'The main reason for writing the book,' says Kashubsky, 'was to fill a specific gap in the literature and provide a useful resource for anyone interested in security issues pertaining to offshore petroleum installations'.

As the self-explanatory title indicates, the book (which started life as a PhD thesis) deals with the increasingly complex issues relating specifically to protecting and maintaining the security of offshore petroleum installations, which include both oil and gas.

Writing in the Foreword, marine and shipping expert Dr. Michael White QC of the University of Queensland remarks that the complex legal questions emanating from offshore security issues are international in nature. So it is useful that part of the book's remit is to deal with the international conventions and the cases that have come before the international courts. In identifying the targets most likely to be attacked, the book explores in detail the regulatory framework and the industry responses to the risks from criminal and/or terrorist violence.

The urgency of the topic and the need for a detailed study of it has become apparent in the wake of the alarming increase in terrorist attacks. 'Oil and natural gas,' says the author, 'account for over 60 per cent of the world's energy supply, one third of which comes from the offshore sector.'

Lawyers, as well as risk management professionals and those doing research into this important subject have, at last, access to a wealth of research resources contained in this one volume. In addition to the copious footnoting, note the selected bibliography and the illuminating appendix of almost- good grief!- 50 pages in length containing tables of attacks on offshore installations dating from 1975 to 2014, (although there was a previous incident in 1899). With its detailed table of contents and index, the book is easy to navigate and there's a useful and lengthy list of abbreviations and acronyms and a table of conventions.

As it summarises the law of the sea as it pertains to offshore zones that are particularly vulnerable, the book will also prove immensely useful for policy makers in government and those professionally involved in the marine and petroleum industries worldwide. Certainly, it should be in every international lawyer's professional library.

The publication date is cited as at 2016.

CSO ALLIANCE –
A COMMUNITY CRIME-FIGHTING PLATFORM

The recent focus on maritime security has spurned the birth of a number of organisations designed to coral and coordinate efforts, improve standards and increase reporting with the ultimate aim of protecting seafarers. We asked our reporter Stephen Spark to look at one of these organisations and share what he found…

For as long as men have been trading across the oceans, they have had to protect cargoes and crews against predatory criminals, from pirates to opportunistic thieves in ports. These days, maritime criminals are well organised and constantly evolving their tactics.

The response from industry and government has sometimes seemed ponderous and piecemeal, hampered by rivalries, secrecy, and a lack of willingness to share information. As the Somali piracy upsurge showed, a ship can be vulnerable if it lacks a clear picture of the threats that lie over the horizon. In such an uncertain world, the job of the company security officer (CSO) can be especially challenging – and isolating.

Late 2012 saw the start of an initiative intended to end that isolation and create a clearer picture of threats to shipping. Mark Sutcliffe (ex Wilhelmsen Maritime Services, Gulf Agency Company) and Robert Twell (who was at the time DPA/CSO at CMA CGM) set up the CSO Alliance (CSOA), which set out to be "a global members-only real-time risk management and information platform for all shipping sectors".

Companies House in the UK where CSO's Alliance is registered shows the company to be structured as a private company with shareholding split between a number of individuals and other companies. One shareholding that stands out is that of Convoy Escort Programme (CEP) Limited, a private maritime security company that had been trying to break in to the industry for a number of years. That company was dissolved in June 2016 after being compulsorily struck off. When asked about its ordinary and preference shares, Sutcliffe commented that CSO Alliance shareholders were considering a change of structure.

To assess how far CSOA has succeeded in its aims, The Bridge spoke to director Mark Sutcliffe last month.

"The criminals are well organised, constantly evolving their strategies. They would love the maritime community to stay disorganised. We want to get everyone working in one world to fight crime," he said. "Working with CSOs, we wish to create a zero tolerance culture to maritime crime."

CSOA provides its members – who have to be verified CSOs or deputy CSOs – with an electronic platform providing a global aggregation of open-source crime reports, from the likes of EUNAVFOR, IMB, MDAT-GoG, UKMTO and RECAAP. Useful as that information undoubtedly is, it is known to be incomplete, because of significant under-reporting.

"We need to improve the reporting of maritime crime incidents to 100%," Sutcliffe said. This is where the CSO members come in, he explained: "Our CSOs are part of a virtuous circle of data and knowledge-sharing." According to CSOA's website, "We collect data from all our CSOs, whether it be a suspected sighting, a stowaway attempt or an opportunistic cargo crime; we track and log every criminal activity anywhere in the world… The platform delivers verified, real-time [reports of] in-port and at-sea incidents and attacks against cargo, crews and ships [using] state-of-the-art geospatial mapping tools."

Other facilities include an online conference and webinar capability, a newsletter, regional workshops and specialised interest groups whose subjects include PMSC due diligence, stowaways, cyber risks and port crime.

All this rests on the electronic platform, developed in-house with Anglo-Dutch outfit Wididi. This month it is being relaunched with improved functionality, particularly for mobiles. Sutcliffe enthused: "We follow our member CSOs' needs and requests for new services so data feeds are being validated, Technology is our friend."

Interactivity is provided by the platform's 'CSO Chatter' forum, which allows members to share and comment on the data. Sutcliffe is keen to stress the 'community' aspect of the Alliance. Fears that disgruntled employees might use it for sniping at companies or rivals are unfounded, he insisted. "To date the CSOs have not used the platform in this way… If this issue did occur we would ensure that no allegation lies unchallenged."

As the organisation approaches its fourth anniversary, it claims more than 400 members "from all ship types and fleet sizes". All are individual members there is no corporate membership option – paying an annual membership fee of £250 for CSOs and £75 for deputy CSOs. This would give CSOA a gross income from subscriptions of £100,000 (if all the CSO's paid the full subscription price). That seems a very tight budget on which to run an international organisation. Enthusiasm for the CSOA offering is strongest in Greece, while Asia accounts for 15% of the total.

If it is such an invaluable service, shouldn't membership numbers be higher by now? Sutcliffe answered: "In the merchant marine deep sea trading fleet there are in the region of 2,000 CSOs and so just under 25%, which is a good start." However, Martin Stopford, in his article on 'smart shipping' in 2015, quotes Clarkson's figures from 2014 indicating that there were "39,000 deep sea ships run by 7,729 companies with an average of 5 ships each". This would suggest there are far more CSOs than CSOA estimates.

"We are a membership community, so this is not a matter of a hard sell." Sutcliffe added: "We grow our membership by word of mouth as well as running CSO workshops." Nevertheless, there are ambitions in the years to come to expand the offering to the 5,000-plus CSOs working in other sectors, such as cruise, fishing, superyachts and ports.

He expects membership to receive a big boost when a deal with the Marshall Islands is completed. "They'd like all of their CSOs to join up. They have several hundred CSOs and want to bring them into this world where they can build a conversation with them as well as others in the profession," he said.

Also in Sutcliffe's sights is the Cruise Line Industries Association (CLIA). An article in CSOA's October newsletter noted: "There are many security synergies to share between the cruise industry CSOs and their security teams and our merchant marine CSOs." The challenge here, Sutcliffe pointed out, is that most cruise ship CSOs come from a police, rather than a maritime, background.

High-profile organisations already on board include North of England P&I Association and BIMCO. The International Chamber of Shipping is said to be supportive. Individual shipping companies are more cautious, it seems: "They like it in principle, but we haven't yet got the message through to management," Sutcliffe admitted. A number of trusted sources across the shipping industry have voiced concerns that their CSOs potentially could make possibly commercially damaging comments that would benefit their direct competitors.

Cyber- crime is just another criminal threat we all face, and as if its existing commitments weren't enough for a still-small organisation to be handling, CSOA is supporting a campaign, backed by North of England P&I Association, called Be Cyber Aware at Sea, which will include a website, posters and an e-learning project.

When asked, the Republic of the Marshall Islands (RMI) Maritime Administrator said it "fully supports the concept of information sharing among CSOs in order to enhance security risk assessments and incident reporting capabilities. CSOs should be working together toward the common goal of safeguarding seafarers, ship owners and operators from physical and cyber-related risks at sea. However, the success of the CSOA concept depends directly on active member participation. Ultimately, CSOs will decide the fate of the platform."

THE MISSION TO SEAFARERS

Caring for seafarers around the world

BRINGING HELP AND HOPE TO SEAFARERS

Today's Mission to Seafarers offers emergency assistance, practical support and a friendly welcome to crews visiting 200 ports in 50 countries around the world.

Whether caring for piracy victims or providing a lifeline to those stranded in foreign ports, we are there for the world's 1.5 million seafarers of all ranks, nationalities and beliefs.

Find out more online at
www.missiontoseafarers.org

or support us on JustGiving at
justgiving.com/themissiontoseafarers.org

themissiontoseafarers @FlyingAngelNews