the BRIDGE

MARCH 2017

MARITME CORRUPTION

BORROWED WEAPONS - THE HIDDEN LIABILITIES TO SHIPOWNERS

END USER CERTIFICATES & GUARDCON

MARITIME CYBER SECURITY: TECHNOLOGY & CULTURE

MARINE HULL INSURANCE IN THE AGE OF AUTONOMY

DRIVING COMPLIANCE THROUGH WEAPONS VERIFICATION

THE MENACE OF SEA MINES

MARITIME TERRORISM

ICOCA - A ROCK AMID SHIFTING SANDS

Welcome to theBRIDGE

Things are changing; the global political environment is volatile and far less predictable than it has been in recent memory. Events in Brussels, London and Washington are having a magnetic effect on the media, hiding many other incidents that are happening across the world. In this issue of theBRIDGE we explore the wide ranging maritime security issues currently having an effect around the globe.

In November last year, BIMCO issued revised Guidelines to their standardised contract GUARDCON, and raised concerns about the "borrowing" and "renting" of weapons by PMSCs in and around the High Risk Area of the Indian Ocean. This situation has been further exacerbated by the closure of the Sovereign Global Services (SGS) Floating Armouries in mid-February. The way in which the private maritime security industry manages this process could be defining and possibly critical to their reputation. We look at this concern from two perspectives, a general review and Stephen Askins provides his legal analysis.

The maritime security industry has for some time been urging the shipping industry to treat cyber security as a realistic threat that will have an impact on business and inevitably cost them money. Many companies across the maritime industry have woken up to the risks whilst others seem to have their heads stuck in the sand. We have two articles in this issue covering this very topical subject; one from a consultant looking at the cultural and technical dimensions of implementing effective mitigating measures and one of the top Admiralty law firms offers their thoughts on how this new menace is likely to affect Hull & Machinery insurance.

Here's a full overview of what's inside this issue...

Pages 4-5

A regular feature in theBRIDGE, the "Global Maritime Security Roundup" highlights some of the most recent maritime security events that have occurred around the world, some of which will be further examined in feature articles.

Page 6

The UK legislation on bribery and corruption, introduced in 2010, was viewed by some as idealistic or puritan in its approach and it threatened to cause the shipping industry significant problems. The "custom" of handing over packets of cigarettes and bottles of Scotch to ease and smooth the process of negotiating certain waterways and docks around the globe was deemed illegal, with the threat of hefty prison sentences. Sandra Spears has been discovering a slightly more realistic and pragmatic approach is being suggested by some parties.

Pages 8-9

From an article originally published in IHS Fairplay, Peter Cook examines the hidden liabilities to ship owners exposed by Private Maritime Security Contractors (PMSCs) borrowing weapons in order to fulfil contracts.

Page 11

Stephen Askins of Tatham Macinnes considers the complexities of weapons usage by PMSCs, examining End User Certificates and GUARDCON.

Pages 12-13

Mike Hawthorne's article Maritime Cyber Security: Technology & Culture explores the reasons why the maritime sector is beginning to embrace maritime cyber security and whether there is a culture and/or technology based solution.

Page 14-15

As cyber attacks become increasingly more frequent and more severe and connected technology becomes ever more present in the physical environment, This feature written by Ricard Murray, Associate Solicitor at Campbell Johnston Clark looks at Marine Hull Insurance in the Age of Autonomy.

Pages 16-17

With the piracy situation in the Indian Ocean waning the price of security is being forced down by the demands of the shipping industry, who are having to manage their bottom line. We have a special feature on Asket Limited, who are driving compliance whilst supporting the shipping industry through weapons verification and ECU tracking.

Page 19

Since a Pentagon spokesman expressed concerns about the threat of sea mines, the US Navy has bolstered patrols off Yemen and sent guided missile destroyers to join the task force defending the Bab El Mandeb Strait. So, should transiting ships be concerned about the menace of sea mines?

Pages 20-21

As the last copy of theBRIDGE was going to press there was a failed terrorist attack on an LNG gas tanker close to the Bab el Mandeb, one of the world's crucial maritime chokepoints. This has been followed up over past few months by further attacks on US and Saudi Arabian warships, whilst a report from the US Pentagon raised concerns of seaborne mines being laid around Yemeni ports in the Red Sea. The threat to this critical waterway is undeniably rising and any closure would have a significant impact on Europe and the USA immediately. We look at the increase in maritime terrorism in the region along with a focus on the use of mines.

Pages 22-23

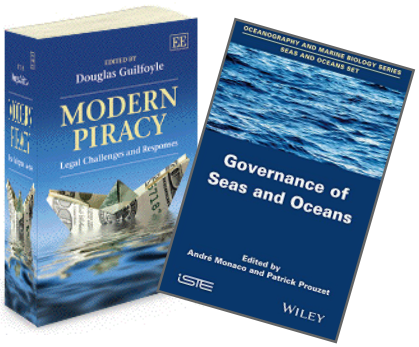
In November 2010, the International Code of Conduct for Private Security Service Providers (ICoC) was launched with great fanfare in Geneva. The code was born of the Montreux Document published in 2008 and both documents were designed provide guidance for nations and contracting companies on how to engage private security companies. The initiatives were timely and the concept was good but the implementation has proved challenging; Stephen Spark provides his perspective on the current status and what's next.

Pages 24-25

In this edition's book reviews, Phillip Taylor MBE and Elizabeth Taylor of Richmond Green Chambers have conducted an appreciation of two books:

Modern Piracy - Legal Challenges and Responses, edited by Douglas Guilfoyle. This book is a three dimensional and analytical look at the menace of modern piracy from legal and academic viewpoints.

Governance of Seas and Oceans, edited by André Monaco and Patrick Prouzet. Legal principles meet environmental science in this important new work of reseearch.



theBRIDGE is published by PCA Maritime

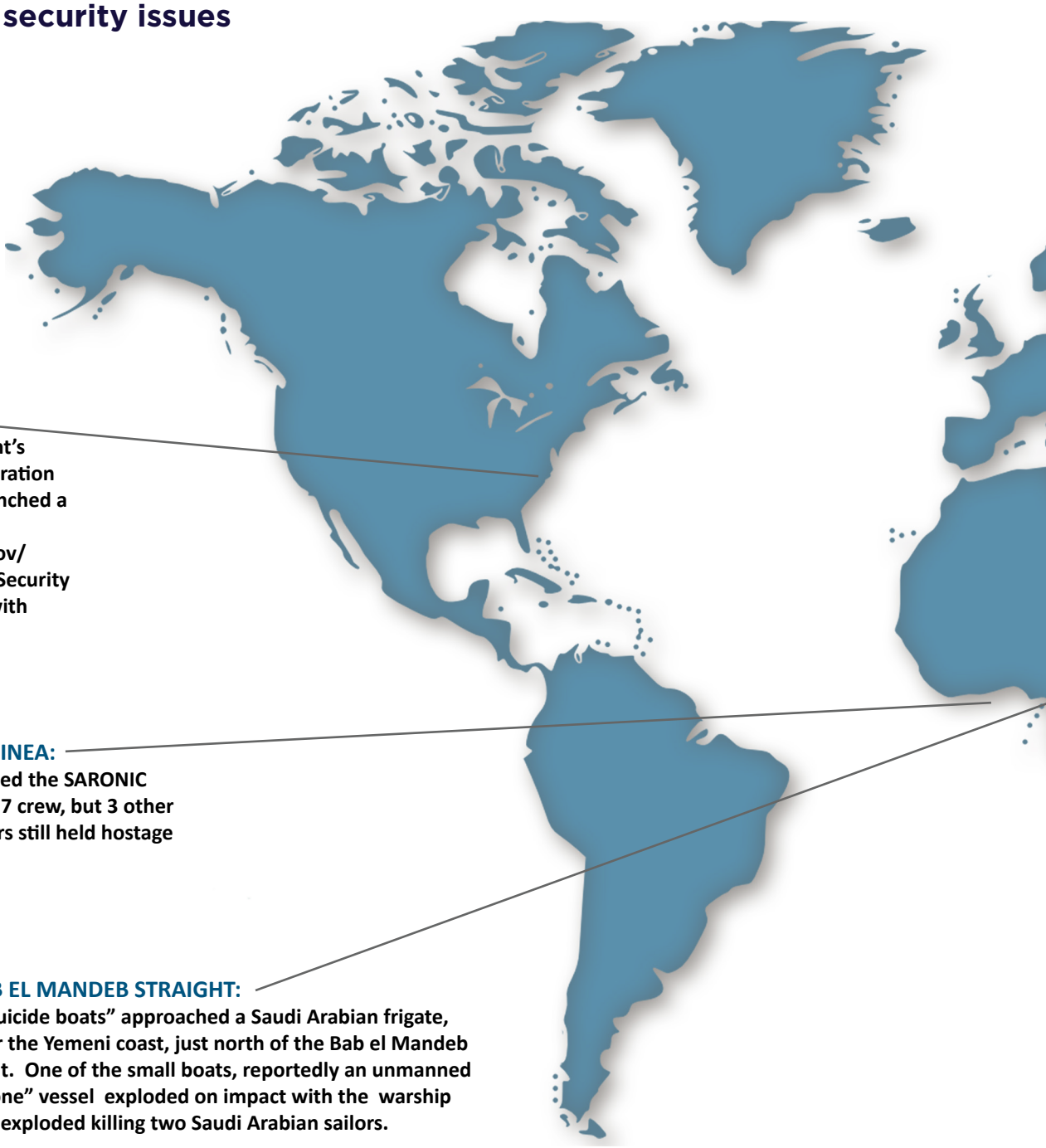
Executive Editors - Peter Cook & Chris Ashcroft

Editorial Contributors - Asket Ltd, Stephen Askins - Tatham Macinnes, Peter Cook - PCA Maritime, Mike Hawthorne - CobWeb Cyber, Richard Murray - Campbell Johnston Clark, Stephen Spark, Sandra Speares, Phillip Taylor MBE

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

Global Maritim

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



USA:
The US Government's Maritime Administration (MARAD) have launched a new Web Portal www.marad.dot.gov/msci for Maritime Security Communications with Industry.

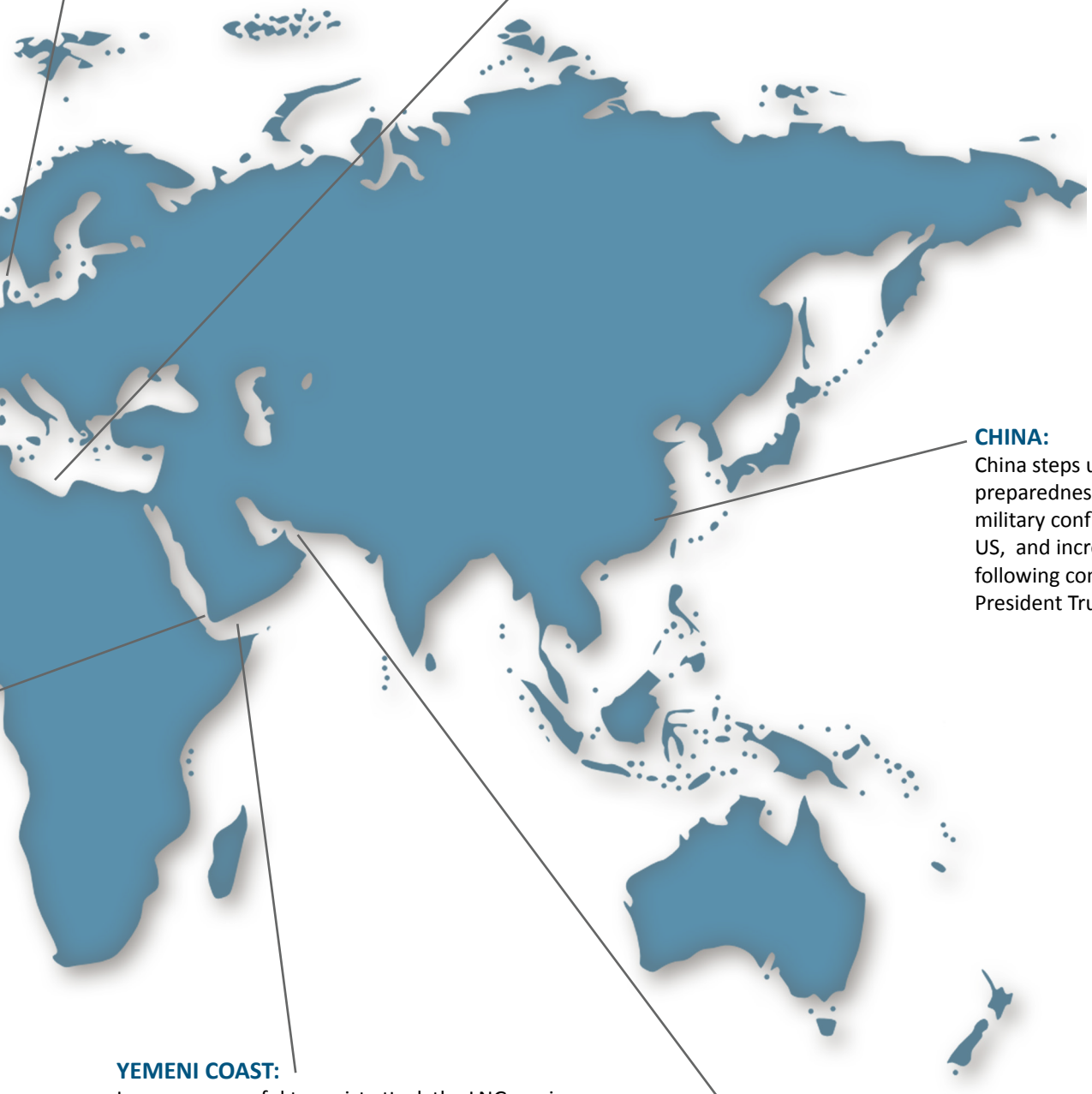
GULF OF GUINEA:
Pirates released the SARONIC BREEZE and 17 crew, but 3 other crew members still held hostage

BAB EL MANDEB STRAIGHT:
3 "suicide boats" approached a Saudi Arabian frigate, near the Yemeni coast, just north of the Bab el Mandeb strait. One of the small boats, reportedly an unmanned "drone" vessel exploded on impact with the warship and exploded killing two Saudi Arabian sailors.

e Security Roundup

DENMARK:
In November 2016 BIMCO publish new Guidelines for GUARDCON highlighting the illegal "borrowing" and "renting" of weapons by PMSCs.

LIBYA:
Training pays off as Libyan Coastguard intercepts 700 Europe-bound migrants 3nm off Sabratha, following exchange of fire with smugglers on beach.



CHINA:
China steps up preparedness for possible military conflict with the US, and increases rhetoric following comments from President Trump

YEMENI COAST:
In an unsuccessful terrorist attack the LNG carrier Galicia Spirit was approached on 25 October 2016 by a single small boat carrying a Water Bourne Improvised Explosive Device (WBIED), which exploded without damaging the ship.

GULF OF OMAN & RED SEA:
Floating Armoury (FA) service provider Sovereign Global Services (SGS) close down their (FA) facilities in the Red Sea and Gulf of Oman reducing the FA capacity by 20-30% and placing significant pressure on PMSCs.

MARITIME CORRUPTION

Bribery and corruption is endemic throughout the world and by no means unique to the shipping industry. In late 2015 BIMCO introduced an anti-corruption clause to charter parties to serve as a blue print for tackling the issue in the maritime arena. Sandra Spears takes a look at some of the effects it has had on the industry.

While the issue is not a new one, the development of the BIMCO clause was triggered by the introduction of stringent anti-corruption legislation including the UK Bribery Act, according to BIMCO's chief officer for legal and contractual affairs Grant Hunter.

TACKLING THE PROBLEM AT GRASS ROOTS LEVEL

Delegates at a recent London Shipping Law Centre Seminar heard that shipping organisations were engaging in direct contact with local governments and bodies, ports and other parties. Working with organisations such as the Maritime Anti-Corruption Network (MACN), which includes a number of key players like oil majors among its members, they seek to tackle the problem at the grass roots level.

"We don't want ship owners being put in such a position of having contracts terminated for situations that are very difficult for them to control," Hunter says. Port delays due to failure to provide facilitation payments could ultimately be used for charter party termination. The key is owners and charterers coming together to resist corrupt practices.

LOW LEVEL CORRUPTION IS STILL CORRUPTION

In many cases it is not a question of money more often a bottle of whisky or 200 cigarettes. Although this is low level corruption, legislation like the UK Bribery Act does not make a distinction.

One important aspect of the BIMCO clause is the ability to protest. If a bribe is demanded from the master of a vessel "he wants to be able to say 'no'" and that protest needs to be logged with the charterers. The protest itself acts as a trigger within the clause, demonstrating that the master and owner have done something to object to the demand and therefore if there is a delay they should not be held responsible.

As Philip Roche of Norton Rose Fulbright pointed out, demands for payment may well be dressed up as something else, for example that the hold of the ship is dirty, rather than a direct demand for a facilitation payment.

According to Nordisk managing director Karl Even Rygh, the clause has been welcomed. However it does not provide a solution to the corruption problem. Mr Roche adds that while bigger ship owners are being successful in resisting demands, this pushes the problem onto smaller owners who don't have the muscle to resist.

FAILING TO PREVENT

The UK Bribery Act scared a lot of people in the industry and not just in the UK, according to Tim Springett of the UK Chamber of Shipping. It included a new offence of failure to prevent bribery, the reach of which is international and includes agents acting for a company.

Chamber guidance has been given on procedures to be followed when a demand for a facilitation payment is received. The maxim is "resist, report, record" according to Springett. In the guidelines it was not possible to give people a "complete 'get out of gaol free' card," he said.

The risk of prosecution remains but the danger has hopefully been reduced. It would appear governments are not providing incentives to companies to report what is happening and the approach is "all stick and no carrot". The consequences of reporting an incident when facilitation payments have been ask for, and paid, can be draconian.

As Philip Roche said the problem is greater for operators of small fleets as against oil majors or big container lines. So what of the master who ultimately is in the hot seat when dealing with demands for facilitation payments? Training is essential Roche says as well as support from the shipping company. MACN, among others supplies this on line to masters and for operators on shore.

Image Credit: Chance Agrella/freerangestock.com

Collaboration Works

Collaboration Works is a concept conceived between Wenford People and Webster Robertson People.

Combining uniquely different & contrasting Shipping Industry backgrounds the two companies are defined by a common vision.

Collaboratively our companies deliver end to end Container Logistics industry expertise as separate components or in packaged solutions.

Collective strength is our “Gearbox”, combining the ability to assess, diagnose and provide solutions for small & large business issues.

Consistent with accepted shipping industry alliances, the Collaboration Works approach to diagnosing business issues results in us providing 360 conclusions and solutions.

wenfordpeople.com **websterrobertsonpeople.com**

THE HIDDEN LIABILITIES TO SHIPOWNERS EXPOSED BY BORROWED WEAPONS!

Peter Cook, PCA Maritime

Since the hijacking of the MT Smyrni in May 2012, no commercial ship has been successfully attacked by pirates and the crew held for ransom in the north-west Indian Ocean. The extremely effective combination of naval forces presence in the High Risk Area (HRA), shipping companies applying best management practices (BMP) and the use of privately contracted armed security personnel (PCASP) – armed guards; has provided an effective deterrent to Somali pirates hijacking ships.

The success of this triad of deterrents resulted in the HRA being significantly reduced in size on 1 December 2015. Consequently, naval forces have been significantly reduced under political pressure, and the application of BMP has relaxed, but the use of PCASP to protect commercial ships transiting the HRA remains at somewhere between 30-50% of ships transiting the area, depending upon which geographical sector of the area you look at.

The Challenge

Providing an effective and efficient maritime armed guard service is primarily about administration and logistics, having the right people (correctly vetted and qualified guards) in the correct location, at the right time, with the correct equipment (weapons, ammunition and security-related equipment) and appropriate documentation to be able to embark a ship in transit for the contracted period of providing the service. The challenge, especially for smaller private maritime security companies (PMSCs), is having sufficient weapons, legally owned by that PMSC, at the point of embarkation, with a team, on time; especially if they work on the "spot market".

The private maritime security industry has consolidated significantly, but remains fluid. It wrestles with the challenges of a perceived reducing threat, a crowded and immature market with some PMSCs negotiating unsustainably low charges for transits, set against international community and shipping associations ever-increasing demand for high standards of compliance.

For a PMSC, moving personnel around the HRA is relatively easy using commercial airlines. However, because many coastal states around the rim of the HRA specifically prohibit the landing of weapons and ammunition, it is almost impossible to move them unless they are being used by a PCASP on task. Consequently, the management of weapons is very challenging and many companies hold up to twice the number of sets of equipment that are used on a regular basis, in order to ensure they can meet the demand.

Proving Weapon Ownership

On the face of it, proof of weapon ownership is quite simple; it comprises three elements; the owner (PMSC), the weapon (each weapon is identified by a unique serial number which is engraved on the weapon in at least two places; the body of the weapon and the working parts). The third critical element that links the PMSC to the weapon is the end user certificate (EUC). The EUC for each weapon, (specified by weapon serial number), will name the PMSC as owner. However, not all EUCs are the same (there is no standard international format), some EUCs list multiple weapons and some countries do not issue them (such as the United Kingdom, but this is supplemented the UK's Open General Trade Control Licence Maritime Anti-Piracy).

Credit: pattanasak kaewhom//freerangestock.com

There are two 'touch points' when the three elements (PMSC, weapon, and EUC) can be verified; firstly, during the contract negotiation. Secondly, when the PCASP and its equipment are embarked onto the ship, normally at sea, mid-voyage.

This complex system is prone to abuse and some PMSCs have overcome the logistical challenges of providing PCASP and equipment by the 'renting' and 'borrowing' of weapons from other PMSCs, which is mostly illegal.

Credit: Jared Davidson/freerangestock.com

New GUARDCON Guidance

In 2012 BIMCO launched GUARDCON, a standard contract for shipowners and charterers to use to contract PCASP, which has proved to be extremely successful and is widely used. In Section 5 of the Explanatory Notes covering permits and licences for the contract it states, "The consequences of contractors failing to have the required permits and licences effectively makes the carriage of weapons illegal". In November 2016, this point was further emphasised in BIMCO's revised guidance, additionally noting that the "ship's flag state needs to see the EUC and verify its authenticity". Failure to do this would breach the contract and thereby cause the ship's insurance to be invalid.

The unauthorised use of weapons is also in contravention of ISO Standard 28007 and the many nations legislation where the PMSCs are registered.

The Floating Armoury Conundrum

An additional factor that potentially exacerbates the problem is the use of floating armouries (FAs). As outlined earlier, many coastal states around the rim of the HRA prohibit the landing of weapons and ammunition. Consequently, a number of entrepreneurs independently developed the concept of placing relatively small vessels (typically offshore support vessels) in strategic locations, with weapon, ammunition and equipment storage capacity, and some accommodation facilities.

The vessels are located in international waters at the corners of the HRA, predominantly in the Gulf of Oman and Red Sea. At its peak, SAMI estimated there were 17-20 FAs in the HRA, each storing around 1,000 weapons, along with ammunition and security equipment. While the international community has expressed concern about this practice, most flag and coastal states lacked the impetus to create an international regulatory structure for FAs, with most states turning a blind eye to the potential risks of not doing so. Because of this apathy, FAs lack any form of centralised control, making it impossible to verify where weapons not on task with PCASP are located.

Inevitably some FAs are managed more effectively and efficiently than others, leading to inconsistencies, confusion and an ideal opportunity for the illegal 'borrowing' and 'renting' of weapons by PMSCs so inclined.

The FA situation was further complicated in early January 2017 when the commercial decision was taken by Sovereign Global Services (SGS), one of the few accredited FA service providers, to close their FAs by mid-February. It is estimated that SGS holds between 20-30% of the weapons, ammunition, and security equipment in circulation in the HRA (including the entire inventory of some PMSCs).

Illegal renting of weapons

The stage is set for a worrying situation to suddenly get much worse. Increasing competition, caused by consolidation in the private maritime security industry, has led to an emerging practice of borrowing and renting of weapons illegally by some PMSCs, which is snowballing. Illegal use of weapons by PCASP breaches contracts and invalidates insurance policies for the ship and the PMSC, increasing the liability of shipowners/charterers and flag states. Without weapon ownership verification conducted effectively, seafarers are exposed to risk and may be vulnerable if something goes wrong, such as an accident with a weapon and ships may be detained in ports.

As problems emerge, solutions appear as well, which will help the diligent flag state, shipowner and charterer to protect themselves from these risks as weapon verification organisations become established. It is too early to know exactly how this situation will develop, but the more proactive are always in a stronger position.

Article originally published in IHS Fairplay: User Certificate Fears Threaten to Sink Floating Armouries, 6th February 2017

http://fairplay.ihs.com/safety-regulation/user-certificate-fears-threaten-to-sink-floating-armouries_20170206.html

Your primary marketing tool is available again…

the BRIDGE is back

A quarterly magazine from PCA Maritime for those in the Maritime Industry engaged in the maritime security sector. the**BRIDGE** is an excellent platform to promote your security services and products.

the**BRIDGE** provides an overview of the most topical maritime security issues and contains news, reviews, analysis, an event guide, business directory and much more.

Distributed digitally, the magazine is also produced in hard copy for distribution at major shipping events across the world and via publication partners. The digital edition is distributed electronically to over 3,000 maritime industry professionals.

the**BRIDGE is published quarterly in February, May, August and November.**

the**BRIDGE** **has a digital circulation of over 3000 with further print distribution at major maritime security conferences and exhibitions.**

Readers include:

- Maritime Professionals
- Seafarers
- Flag States
- Marine Insurers
- Lawyers
- Classification societies
- Regulators
- Ship owners &managers
- Security Professionals
- Jobseekers

the BRIDGE

WWW.PCAMARITIME.COM

End User Certificates and GUARDCON

Stephen Askins of Tatham Macinnes looks at the complexities of weapons usage by PMSCs

In BIMCO's recent amended guidance on Clause 10 of GUARDCON it states that there are a "small minority" of private maritime security companies ("PMSCs") that are using weapons borrowed from another PMSC. Some of the PMSCs flip this on its head and suggest that it is actually only the small minority that do not lend or borrow equipment. Tellingly BIMCO goes on to say that this is being done "to save operating costs and undercut legitimately operated PMSCs". It has to be assumed that BIMCO are not seeking to extend their remit to defend the interests of the "legitimate" PMSC world and must consider it still to be in the owners' interests to have armed guards. That means the sector cannot be undermined to the extent that it is not commercially possible to provide the guards the market requires. However, BIMCO have suggested that this practice can be overcome by further due diligence being done by owners (and presumably the master) by checking the End User Certificates which must accompany each weapon.

End User Certificates

A lot of effort is made internationally to ensure that small arms and light weapons do not reach conflict zones or embargoed countries. That is best done through the denial of export licenses of which the issuing of an End User Certificate (EUC) is an important part. There is no uniformity over what an EUC should be although there are international protocols and agreements which specify the information which should be included although again most of those are aimed at government EUCs rather than private ones. The system is open to abuse.

The problems for the ship owner arise when an audit is done by a port authority and the EUC is found to have been issued to a different PMSC from the one providing the services on board and the vessel is detained and delayed as result. Clause 10 of GUARDCON provides for mutual obligations on each party to "obtain and maintain all Permits which may be required" to allow the vessel to have armed guards on board and for those armed guards to have weapons. "Permits" as defined is wide enough to include all certificates and therefore covers EUCs. The definition also covers "authorisations, permissions [and] approvals". The issue then is who bears the risk of any delay caused by having an incorrect EUC. Ordinarily one would be confident to conclude that this is an obligation on the PMSC. However, the new BIMCO guidance confuses the situation by stating that "it is a legal obligation [arising under a number of relevant conventions] on flag states and they should be sighting and verifying EUCs as a matter of routine".

Whose responsibility?

If that is right and there is a Convention based obligation on flag states (and the basis for that assertion is not at all clear) to inspect EUCs then that would appear also to be a potential Owner's obligation under Clause 10 (a). That was not what was in the minds of those drafting GUARDCON. A valid EUC feels like it should be a matter for the PMSC. That confusion and potential point of conflict would sensibly be overcome by an additional clause making it clear that having a valid EUC is a Contractor's obligation or alternatively they should be listed in Box 11 of the GUARDCON as one of the Permits that the Contractors has obtained. Assuming that is clarified then the risk of delay and other losses will fall squarely on the Contractor. Clearly an owner will want to avoid delays but increasingly as part of the due diligence process they are being asked to delve ever deeper and with greater understanding into the Contractor's documentation.

At the end of the day many of the Contractors will also be Associated Members of BIMCO and yet it is not at all clear what due diligence is done by BIMCO to determine whether their members are potentially undermining fellow members. The identity of those who do lend and borrow weapons are probably known and a robust peer review would probably identify most if not all of them and having determined that they were acting illegally it would then be for BIMCO to decide whether they should still be associated members. The risk of being exposed in that way maybe a much more effective way to prevent the undermining of legitimately operated PMSCs.

MARITIME CYBER SECURITY: TECHNOLOGY AND CULTURE

The International Ship and Port Facility Security (ISPS) Code provides a framework through which ships and port facilities can co-operate to detect and deter acts which pose a threat to maritime security. This framework quite clearly addresses culture and technology issues. At the same time, organisations like the IMO, the American Bureau of Shipping and the Institute of Engineering & Technology are publishing guidelines on maritime cyber security. All three highlight potential culture and technology options for improving cyber security. This article will explore the reasons why the maritime sector is beginning to embrace maritime cyber security and whether there is a culture and/or technology based solution.

The Forth Industrial Revolution

Klause Schwab of the World Economic Forum argues that we are in the fourth industrial revolution – the emergence of cyber physical systems – and Eric Brynjolfsson in his book the "Second Machine Age" argues a massive technological innovation is radically reshaping our world- the significant contribution that mastery of digitisation will bring to delivering competitive advantage. What is clear from both books and from our broader reading is that the world is becoming increasingly reliant on digital technology. This applies to the maritime sector too.

In the maritime sector, the emerging paradigm is a data-centred business model directed by a data-driven decision making process. In the past, a ship was operated with significant autonomy as a "stand alone" unit, now a fleet of ships can be managed as a single business unit. This new paradigm is underpinned by several factors: the ubiquity of "big data" and the associated challenges of working with structured and unstructured information, cheap data storage and the use of passive and active (smart) data, and finally increased use of machine learning algorithms to support greater automation. Around the world, organisations that dominate their sectors have deployed industrial strength analytics across a wide variety of functions in order to drive efficiencies into their business processes and to minimise costs. This has already become the norm in the maritime sector. The benefits are clear. The ship operator can monitor and interact with every aspect of maritime operations: ship to shore communications, proactive management of maintenance schedules, optimise loading manifests and the processing of management data into a useable form which supports more effective decision making. This has led to improved productivity, better quality control and increased reliability. We all know there is a cost: a cost in transforming the business processes and a cost in managing the security concerns that digitisation brings. These increased efficiencies in our working environment have led to more cyber vulnerabilities across our lines of operation.

Challenges and Lessons

The challenge for us all is to identify how to manage the increasingly digitised maritime environment, how we should respond to the increasing cyber vulnerabilities and what is the optimal mix of cultural and technology interventions. Although most cyber attacks in the maritime sector are not declared in public forums, due to market sensitive reasons, some were declared in 2016 albeit with limited detail. For example, we have seen the specific targeting of shipping containers by pirates in order to identify high value cargo and the theft of a $10 million deposit on a ship order enabled by a Cyber Fraud attack. The main technical lessons that were identified from the piracy attack included the requirement for more regular vulnerability scans and more formal software patching processes. Like most cyber fraud attacks, "phishing" emails played a significant part.

But both attacks would have had cultural aspects including poor maritime cyber hygiene and poor awareness of the cyber security vulnerabilities by employees. Cyber security is a holistic discipline. It requires robust technical solutions that ensure critical systems are well protected, documented policies and process controls that ensure "best practice" is fully implemented, and effective management and training of employees, including vetting of staff in critical posts, the implementation of the "least privilege" discipline to minimise the consequence of any security shortfall and a more mature understanding of an individual person's role in cyber security.

Credit: Tashatuvango/Shutterstock.com

A Physical Comparator

The maritime sector has an embedded and instinctive understanding of watertight integrity. Watertight integrity can be breached through any activity or event that allows the ingress of water in unwanted areas or compartments of the vessel. It is the individual responsibility of all employees, visitors, contractors and clients to be aware of how watertight integrity might be breached. In the same way the maritime sector should demand an instinctive understanding of maritime cyber security. The integrity of cyber systems could be breached through any activity or event that allows unauthorised access to computer systems supporting critical functions, either control functions or data flows. It is the responsibility of all maritime employees, visitors, contractors and clients to be aware of how cyber security might be compromised. The approach to delivering the required security posture will be shaped by a combination of technical and cultural activities:

- Cyber Awareness training including specialist and for all
- Information Technology and Operations Technology Risk Management
- IT and OT Assurance
- Intelligence
- Secure Networks
- Secure Systems
- Secure Applications

As the ISPS Code has technical and cultural dimensions, similarly maritime cyber security has both cultural and technical responses. The challenge for us all, in this unregulated environment, is identifying the appropriate response. A good place to start is to take full advantage of the available guidance (ISO 27001, NIST Cyber Security Framework, BIMCO Guidelines, etc), seek out best practice and to develop a security posture and risk appetite that is appropriate for your particular operational circumstances.

Mike Hawthorne *OBE MSc MA FBCS FCMI is a former Captain in the Royal Navy and is now COO at CobWeb Cyber. He has a unique understanding of Cyber Security, including cyber risk management of Enterprise and Operations Technology Systems. His passion is leading Change Management Initiatives that enable improved Cyber Security.*

Marine Hull Insurance in the Age of Autonomy:
From Cracking to Hacking

Two closely related technology stories, rarely mentioned together, characterise the cyber threat at the start of 2017.

First, cyberattacks are becoming increasingly more frequent and more severe; from elaborate phishing scams and data leaks affecting millions of consumers and businesses, to the alleged infiltration of a US presidential election.

Second, society is willing to allow, with little if any resistance, the introduction of connected technology into the physical environment; the testing of driverless cars, rapid developments in the use of drone technology, and the exciting (or terrifying) prospect of autonomous shipping.

Credit: Alex Kolokythas Photography/shutterstock.com

Defending the Hackable

On the one hand, governments and businesses are continually trying to defend themselves from cyber threats, while on the other, inventors introduce ever more hackable technology into the marketplace. The overall "attack surface area" is dramatically increasing. From the prudent underwriter's perspective, the risk outlook is not very appealing. If you are in the business of insuring buildings against the risk of fire, there is comfort from the fact that modern construction and H&S regulations have come a long way since the Great Fire of London in minimising a risk that is now easily calculable, albeit not unavoidable.

With good reason, there will always be cyber non-conformists. Many intelligence services will continue to keep their most valuable treasures on paper only; locked in heavy safes and dark basements. Perhaps the very definition of un-hackable.

In a similar vein, many ship operators remain unconvinced by the safety of electronic bills of lading, preferring the reassuring individuality of a signature and the company seal to approve/endorse contracts of carriage.

However, put any piece of information or control system onto a device connected to a network, and risk analysts find themselves within a global cyber threat environment.

Traditional Assumptions Challenged

Traditionally, the underwriting of physical losses has worked on the assumption that most physical damage requires physical proximity. Therefore, the market has been preoccupied with the contact between ships and other tangible processes in the natural and human environments, such as human errors of navigation or fortuitous "acts of god".

However, these assumptions will be challenged as ships become more globally "connected", and potentially autonomous. Cyber risks are typically universal rather than local, non-physical, and without warning; making them less calculable for insurers, who are concerned that certain types of cyber risk could lead to multiple or endless losses from a single incident.

The Advanced Autonomous Waterborne Applications Initiative (AAWA) supported by Rolls Royce anticipates that commercial shipping will have a remote-controlled vessel in use by the end of the decade. Amongst other factors, the opportunity for ship owners to improve profit margins by reducing labour costs may determine the concept's long term appeal.

Commercial Pressures

The insurance market will, in turn, face commercial pressure from ship owners to expand coverage on cyber risks, which would modify the contractual relationship between underwriters and ship owners under marine hull policies. For example, this might involve a relaxation of the commonly seen Institute Cyber Attack Exclusion Clause, or a redefinition of All Risk cover to underwrite a certain level of cyber risk within carefully worded limits, rather than issue an outright exclusion.

Autonomous shipping will also redraft regulatory frameworks. For example, what should competent seamanship look like if the Master/crew are not on board the vessel? Underwriters will also take a keen interest in how classification societies can respond to and manage the technical requirements of autonomous ships.

In the event of a coverage dispute between owners and insurers involving an autonomous vessel, these regulatory issues will in turn challenge certain long established norms of what is understood, under English insurance law, to be a "seaworthy" vessel.

Should an autonomous vessel be rendered legally unseaworthy, if involved in a collision resulting from a loss of navigational control after a cyber-attack on systems with out of date fire wall software? Will charterers be in breach of their unsafe port/berth warranty in the charter party, by nominating a port/berth without the shore capabilities to handle a particular model of autonomous vessel? Factual scenarios like these have never been seen by the courts before, and would need to be treated on a case by case basis.

Seaworthiness

The English courts are traditionally pro-active and commercially conscious when it comes to applying existing legal principles to new technologies. Hypothetically, in the event of a vessel loss by cyberattack (or systems malfunction), there is no reason why, in principle, the implied warranty of seaworthiness under existing insurance law should not remain relevant, notwithstanding the absence of a Master/crew on board.

Of course, the process of investigating marine claims to determine whether an autonomous vessel was "reasonably fit in all respects to encounter the ordinary perils of the sea" (see s.39 Marine Insurance Act 1906), from an evidence gathering perspective, would change significantly. 'On-land' watch keeping practices could expect to be carefully scrutinised, vessel logs will record a host of new data to be analysed, an army of forensic IT specialists may find themselves in high demand, and class/port state control records subjected to the rigour of expert testimony.

While the future of autonomous shipping will present challenges for owners and underwriters alike, both the market and the rule of law will, as it so often does, test and adjust accordingly.

Richard Murray is an Associate Solicitor at Campbell Johnston Clark ("CJC") and specialises in marine insurance and admiralty litigation. He joined the firm in 2013 after beginning his career in the maritime security industry, and was called to the Bar in 2016. He is also a reservist in the British Army.

CJC is a market-leading practice with offices in London, Newcastle and Singapore, and provides a full legal service to the shipping & offshore industries.

DRIVING COMPLIANCE & SUPPORTING THE SHIPPING INDUSTRY THROUGH WEAPONS VERIFICATION & EUC TRACKING

With the piracy situation in the Indian Ocean waning the price of security is being forced down by the demands of the shipping industry, who are having to manage their bottom line. Security companies fighting for transits are undercutting each other and many are taking short cuts that put the vessel, crew and operator at serious risk.

One company trying to drive compliance whilst supporting the shipping industry is Asket Ltd. Through its Approved Provider list Asket carefully vets PMSCs, whose services are then brokered to clients requesting armed security for a transit or transits. Each PMSC is monitored on a transit by transit basis across client fleets to ensure continuous compliance, helping to eradicate unscrupulous PMSCs that might be undercutting the costs of legitimate security providers, and thereby helping to raise standards across the industry.

Asket's bidding process allows the shipping company CSO to compare the service offered and pricing on a like by like basis across a number of PMSCs from the Approved Provider List. Information provided includes a statement and check of insurances, team credentials and weapon licences for each individual transit.

Using their in-house Weapons and Licence Database Asket can check serial numbers, licences and End User Certificates for the ship owner and flag State, helping to mitigate their liability in the event of a firearms incident, as emphasised in BIMCO's updates on GUARDCON. This also eliminates the possibility of illegal sharing of weapons by any PMSCs contracted via ASKET

Through stringent checks ASKET has uncovered instances where PMSCs are operating illegally, including weapons sharing and renting, and other practices such as taking weapons into UN Sanctioned countries, and boarding vessels without flag State clearances - all of which put a vessel at risk of detention and likely invalidating its insurances.

Asket boasts impressive statistics with a recent survey reporting that 80% of its client ship owners and managers saved both time and money using its brokerage services.

ASKET's free resources, in particular their Maritime Security App, were recognised when the company became finalist in the Lloyds List North America Awards 2016.

As part of a holistic approach to consider the strategic and long term concerns of flag States, Maritime Governing Authorities and Organisations Asket is now working closely with PCA Maritime Ltd. Together they aim to provide the most relevant and best maritime security support possible to the shipping industry on a Global basis.

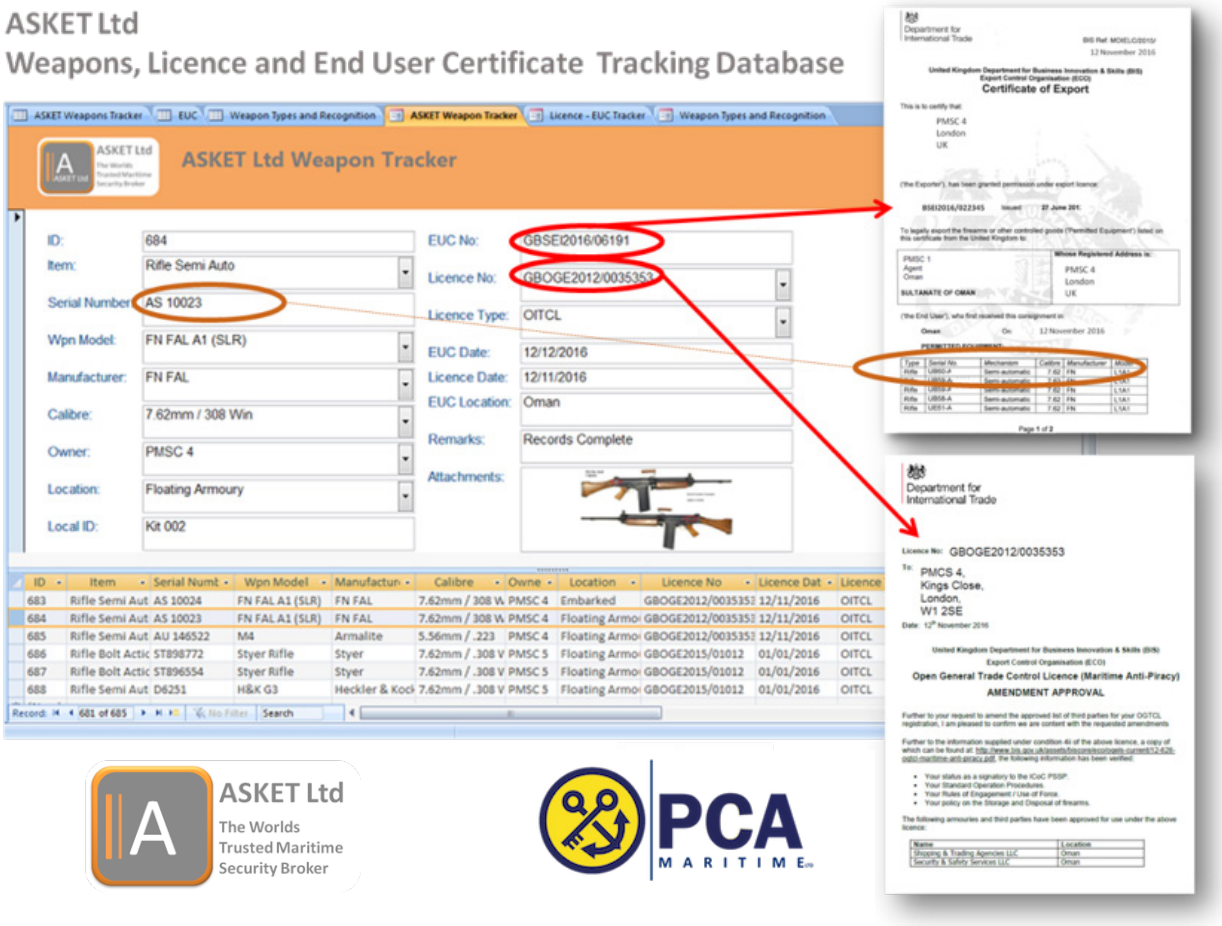
ASKET Ltd is the world's leading fully independent maritime security brokerage, established in 2013 to support an industry being hammered by low rates and costs of manpower, time, insurance and armed guards.

Asket's team works in direct support to ship operators and has a wealth of experience including, team leader during an armed pirate attack, compliance and recruitment, and Risk Management leadership in a global insurance broking house in the London Market.

Driving quality and compliance Asket reduces many of the risk, time and costs associated with the contracting of Security Providers in the Indian Ocean and West Africa.

Emma Mitchell is Director of Business & Compliance at Asket. She studied Criminal Law before working for a Global Security Company and PMSC. After seeing the way that some security companies were failing the shipping industry, Emma co-founded Asket in 2013, with the aim of supporting ship owners and CSOs in the procurement of professional maritime security services.

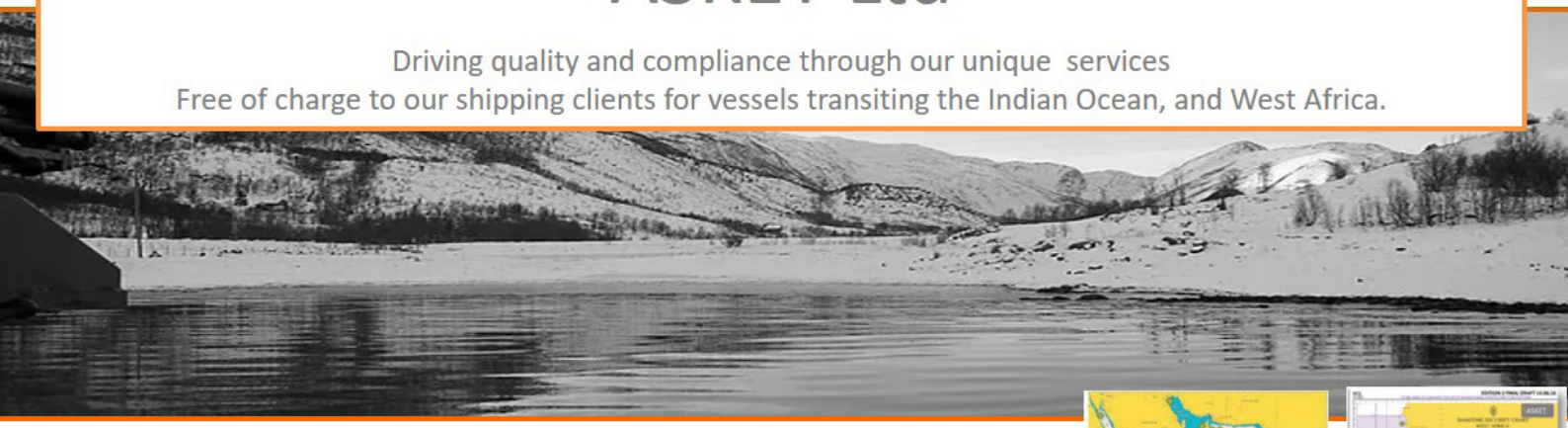
www.asket.co.uk



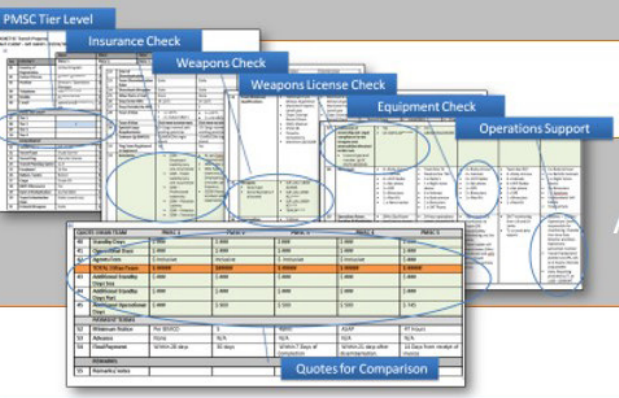
Asket's in-house Weapons and Licence Database can check serial numbers, licences and End User Certificates for ship owner and flag States, helping to mitigate liability in the event of a firearms incident.

ASKET Ltd

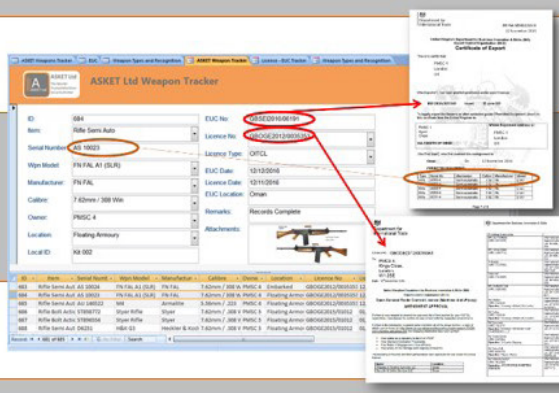
Driving quality and compliance through our unique services
Free of charge to our shipping clients for vessels transiting the Indian Ocean, and West Africa.



Offering impartial comparison quotes in just a few clicks



Approved Providers - Pre Vetted - Transit by Transit Monitoring



Broking process - Weapons data base – Licence & EUC Checks

Free Resources - Monday Briefing - Flash Alerts - Maritime Security App

Free Services Include

- Support to CSO's and Vessels transiting the Indian Ocean and West Africa
- Access to Vetted Approved Providers
- Selection of quotes in one form to allow CSO's to compare like for like
- PMSC declaration of insurances, licenses and certificates for each transit
- Transit by Transit Monitoring of PMSCs
- ASKET Weapons Data base check
- License and EUC Checking
- Monday Briefing & Flash Alerts
- Maritime Security App
- Operational advice, guidance and Training Resources

ASKET Ltd- The Worlds Trusted Security Broker
Web: asket.co.uk Twitter: @asket_broker Tel: 0044 7827 012 195

THE MENACE OF SEA MINES

As the US Navy bolsters forces patrolling off Yemen, a Pentagon spokesman has expressed concerns about the threat of mining. The Arleigh Burke Class guided missile destroyer USS Cole has joined the task force defending the Bab El Mandeb Strait amid worries that Houthis may try to block the maritime choke point with sea mines. Reports in the US press quote Capt. Jeff Davis stating that there is evidence of Houthis laying mines in waters off at least one port. So, should transiting ships be concerned?

MINES ARE RELATIVELY CHEAP

Sea mines have been part of the maritime landscape for a long time. A simple contact mine that relies on chemical "initiator" to detonate a charge when it is struck by a ship can be manufactured for as little as $50, as the Iraqi's showed in 2003.

The Red Sea and Bab El Mandeb Strait are part of a vital route that sees maritime trade flow from the Middle East to the West, via the Suez Canal. The closure of this route, whether through mining or increased attacks on shipping, would seriously undermine the supply of oil and gas, adding over 15 days to the journey from Fujairah to the Gibraltar Straits – days that cannot be made up simply by adding more vessels to the supply chain as there are not enough tankers lying idle to fill the gap.

OFFENCE IS THE BEST DEFENCE

The key to protecting against the threat of mines is to prevent them from being laid in the first place – the perfect example of the best defence being offence – finding and destroying mines before they enter the water. Immediately before the invasion of Iraq, in March 2003, the Australian Navy intercepted several converted non-military vessels carrying over 80 mines, including sophisticated Italian electronic mines and more rudimentary home-made Iraqi contact mines. Laying mines in sufficient quantity to close the Bab El Mandeb Strait would require a significant logistical effort that would be susceptible to detection and disruption. Nonetheless, even the threat of mines and the perception of the risk posed to shipping even if only a few were laid could impact the insurance premium rates set for ships transiting these waters.

The US Navy is right to be concerned as mines have damaged more US naval ships than any other weapon since World War II. Fifteen vessels have been sunk or damaged, almost four times more than by any other weapon.

MILITARY PREPAREDNESS

From a military perspective, with the levels of surveillance in and around the area, it is hard to see how Houthis could conduct a serious mining campaign out in the Bab El Mendeb Straits. Several nations have mine countermeasures vessels in or close to the area, including Saudi Arabia, the UK and the US, so in the event of actual mining action the international community could respond quickly and effectively. The perception of a risk averse Hull & Machinery Underwriter may not share the same view.

WHO WINS?

One important question is who would be served by such a campaign? The Chinese are the world's largest importer of oil and would certainly not wish to see supplies interrupted or reduced by tankers having to be diverted to move oil West – in this respect their interest is aligned with the US, oil and gas must continue to flow. Though Iran backs the Houthis, it is desperately trying to re-set its economy so that it is again allowed to export, and any hint of involvement in a mining campaign would probably attract considerable attention from the West, particularly the US. Perhaps the country to gain most would be Russia, as Western Europe would almost certainly have to increase imports of gas through the Russian pipelines if the umbilical cord to Middle Eastern oil and gas was cut.

During the tanker war of the 1980's between Iran and Iraq, super-tankers were escorted in convoys, usually in single file, and relied on their sheer size to push mines aside and to keep afloat in the event of a strike. When Egypt closed the Suez Canal in 1967 the size of tankers increased massively to close the gaps on demand. These days tankers are double-hull constructed and would be unlikely to sink after just one strike from a contact mine. Similarly, this construction helps to reduce the impact of pollution and environmental damage.

So, should transiting ships be concerned? Probably not concerned, but at least wary and watchful.

MARITIME TERRORISM

Credit: Katarzyna Mazurowska/shutterstock.com

Maritime terrorism in the southern Red Sea and Gulf of Aden is real. Whether State sponsored or ideologically motivated, the attacks are growing in tenacity and audacity. Whilst some will debate what the target was, these attacks are happening in the area of the Bab el Mandeb Straits, one of the busiest maritime chokepoints in the world, making it increasingly dangerous for the hundreds of merchant ships passing through every week.

Most recently on Monday 30th January three "suicide boats" approached a Saudi Arabian frigate off the Yemeni coast, north of the Bab el Mandeb. Whilst details were unclear at the time of going to press, it would appear from the video posted online, that one of the boats carrying a waterborne improvised explosive device (WBIED) collided with the rear of the warship and exploded, reportedly killing two Saudi Arabian sailors.

On 25th October, last year the LNG carrier GALICIA SPIRIT was in the mouth of the Red Sea, close to the Bab el Mandeb when a small boat exploded close to the vessel, suggesting that the craft's mission was a suicide attack. The boat was packed with explosives "sufficient to have caused significant damage to the vessel" said the ship owner (Teekay).

Whilst we cannot be certain about who was responsible for either attack, they demonstrate a clear increase in daring and development of tactics by those who carried them out.

This asymmetric modus operand has been utilised by terrorists in the region before. In 2000, the USS Cole was almost sunk when a suicide bomber driving a small boat detonated a WBIED, killing 17 US Navy sailors and injuring a further 35 in the port of Aden. In 2002, the MV Limburg, a Suezmax oil tanker, was attacked by a suicide bomber with a WBIED at sea, in the Gulf of Aden; demonstrating a development of capability and boldness. In 2010 the M Star, a VLCC, was attacked in the Straits of Hormuz and, whilst it is acknowledged that the attackers were terrorists using more than one boat and a WBIED, the details remain shrouded in mystery.

Al Qaeda (AQ) has been exploring maritime terrorism opportunities for some time and in October 2014 AQ used its propaganda publication to urge attacks on the "Achilles Heel of Western Economies" stating that "if a single super tanker were to be attacked in one of the chokepoints or hijacked and scuttled in one of the narrow sea lanes the consequences would be phenomenal".

Some commentators have dismissed the likelihood of a terrorist attack at sea, saying that without televisual coverage they are starved of the "oxygen" of publicity they crave. However, as we have seen, terrorists will utilise the latest commercially available technology to film their attacks and distribute the footage on YouTube, exploiting social media to publicise the incident to ensure as it goes "viral". This is a far more immediate, dynamic, shocking and globally all-pervading than a scheduled report on Aljazeera/BBC/CNN.

A successful missile attack, almost destroyed the UAE flagged HSV-2 Swift on 1st October 2016, and was followed by several other confirmed and unconfirmed attacks on US warships in the same area. Though these attacks were obviously not directed at commercial vessels they cannot be ignored.

To add another dimension to the potential danger in the region, on 4th February, a spokesman from the US Pentagon announced:"We've seen evidence that Houthis are laying mines in the waters outside at least one of their ports. We officially have a great concern for the freedom of navigation there"

This can only add to shipowners' flag States' and insurers anxieties about transiting this area. After all, who would want to walk into a bar where there's a punch-up in progress to get a drink?

The recent increase in terrorist incidents, successful and unsuccessful, clearly demonstrates intent; the use of multiple boats is tangible evidence of an evolving capability. The reduction in naval warships in the north-west Indian Ocean seems to have provided the opportunity. Maritime terrorism is not just an idea, it is an audacious reality that, if allowed to go unchecked, could have a massive impact on the "Achilles heel of Western economies".

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

Stephen Spark takes an in-depth look at **ICOCA - A rock amid the shifting sands?**

The past decade has seen increasing complexity in security environments matched by a similar complexity in the measures taken to address those security challenges. In response to widespread concerns from governments, civil society organisations (CSOs) and activists, many of the new measures have been designed to ensure that private security companies (PSCs) not only sign up to a commitment to apply human rights and humanitarian principles in their work, but also demonstrate that commitment through auditing.

This has led to a somewhat confusing proliferation of standards, with inevitable gaps, overlaps and duplication. It is, perhaps, to be expected in this period of transition both in the threat environment and in the legal and practical responses to it.

Geneva base

Nowhere is this demonstrated more clearly than in the still-evolving International Code of Conduct for Private Security Providers' Association (ICoCA), based in Geneva. It is no coincidence that the Swiss city is also the headquarters of the Geneva Centre for the Democratic Control of Armed Forces (DCAF), which was founded in 2000.

Along with the Red Cross and the Swiss Federal Government, DCAF developed the 'Montreux Document', which laid down that private military and security companies involved in armed conflicts should respect international humanitarian law and human rights. It also provides guidance on good practice in situations not involving armed conflict. It is not legally binding, although last year DCAF produced *a Legislative Guidance Tool for States to Regulate Private Military and Security Companies*, which aims to help States produce their own national legislation.

Seventeen countries signed up in 2008 to T*he Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict* (to quote its unwieldy full title). Estonia's signature in July 2016 brought the total to 54 states, plus three multinational groupings: the European Union, NATO and the OSCE.

No force of Law

The Montreux Document was clearly valuable groundwork, but it was never going to satisfy those who cited high-profile abuses such as the September 2007 shooting of civilians in Nisour Square, Baghdad, as examples of private armed security personnel apparently being above the law and out of control. By not having the force of law or certification behind it, the document could not give much assurance to those who contracted security personnel who needed to know whether they were truly compliant with the best international standards on human rights, rules on the use of force and appropriate business conduct. Nor did it help responsible security providers prove they were putting into practice these good intentions and thereby distinguishing themselves from less disciplined operators.

Two years after the launch of the Montreux Document, the International Code of Conduct for Private Security Providers (ICoC) was developed. Like Montreux, the Code is built around the 'Respect, Protect, Remedy' framework developed by UN Special Representative John Ruggie in 2008.

The Code's Preamble notes: "The activities of PSCs can have potentially positive and negative consequences for their clients, the local population in the area of operation, the general security environment, the enjoyment of human rights and the rule of law." It is largely land-focused, leading IMO to conclude that ICoC offered little that was not covered in its guidance on the use of onboard privately contracted armed security personnel (PCASP) as set out in MSC.1/Circ.1405 (*Guidance to shipowners, ship operators and shipmasters*) and MSC.1/Circ.1443 (*Guidance to private maritime security companies*).

Signatories flock to the Code

By the time the ICoC was completed in November 2010, 58 private security companies had signed up to its requirements for good governance, respect for human rights and international humanitarian law, and a high standard of professional conduct. By September 2013, that number had grown to 708, despite (or perhaps because) a signatory's practical application of their commitment not being subject to independent scrutiny.

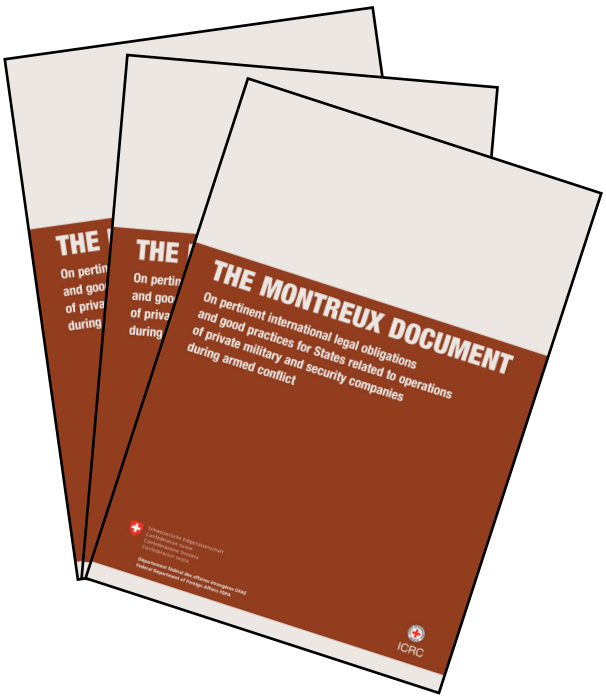
Recognising that it was an important step forward in regularising the standards required of PSCs, the Security Association for the Maritime Industry (SAMI) required all its members to sign up to the Code.

SAMI's endorsement gave a boost to the next stage, which was to formalise the Code's steering committee as an association. Hence, in September 2013 International Code of Conduct for Private Security Providers' Association was established as a Swiss non-profit organisation. The UK Government provided £300,000 initially, and other states also provided funding.

Signatories were invited to join the association, and naturally SAMI members accounted for a significant proportion of ICoCA's 135 founder members. In contrast to purely industry-based associations, ICoCA comprises three pillars: PSCs, governments and civil society organisations (CSOs). Currently, there are 91 industry members, and about half of these include a maritime security capability. UK-headquartered companies remain the biggest single group (21), followed by the USA, with 14 PSC members. There are 18 CSOs, six of which are in the USA, and seven supporting governments. The six founding states were Australia, Norway, Sweden, Switzerland, the UK and the USA, while Canada joined on 13 December 2016.

Failing companies and membership costs contribute to declining membership

The decline in membership from September 2013 to January 2017 is attributed to a number of PSCs going out of business or merging. Some industry observers have suggested that the benefits for smaller PSCs do not outweigh the cost of membership dues and initial joining fee, although the dues are on an earnings-based sliding scale.



An ICoCA spokesman told 'theBRIDGE' that until now it has not formally invited companies and organisations to join, so most recruitment has been through recommendation. He pointed out that the focus is on PSCs operating in 'complex environments' rather than those providing routine security in stable situations – perhaps explaining why ICoCA members are not among the UK's top 30 (by 2015 turnover, according to www.infologue.com). The Association's website shows that 14 PSCs and four CSOs joined last year.

First ICoCA Certification

A notable milestone was reached in December 2016 when Olive Group became the first PSC to achieve ICoCA certification – although the following month it became part of US-based Constellis.

Certification requires a PSC to gain third-party accreditation to at least one of three standards: PSC.1-2012, ISO 18788:2015 and ISO 28007-1:2015. The latter is the standard for provision of PCASP on board ships and, for ICoCA certification purpose it is accompanied by an annex, "because certain additional information relevant to the human rights and humanitarian impact of operations is necessary for the Board to assess whether a company's systems and policies meet the requirements of the Code".

From September 2018, certification will be compulsory for all members. ICoCA warns: "Companies that signed the Code but have not applied for membership are no longer fulfilling their commitments as signatories."

Does ICoCA go far enough?

Critics, such as War on Want's executive director John Hilary, say that these provisions do not go far enough, as auditing relies on self-assessment rather than the force of law and third-party scrutiny. So long as compliance with the ICoC is voluntary, they argue, the industry is effectively unchecked.

That ignores the commercial impetus behind compliance and certification: the need to be able to prove to nervous potential clients that they are not about to have their reputations sullied or their organisation or government tied up in lawsuits by employing trigger-happy cowboys. In an increasingly competitive field, PSCs have to be able to distinguish themselves from those whose services are merely cheap.

Is ICoCA achieving enough? Its spokesman pointed out: "We're still a relatively young organisation. Our procedures have only been online since September." In the ever-shifting sands of security provision and standards in complex environments, he added, "We hope that we'll be able to become a bit of a rock."

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

Book Reviews:

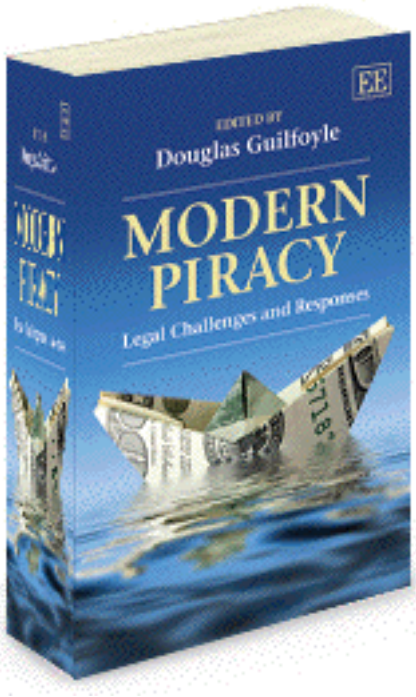
Modern Piracy
Legal Challenges and Responses

Edited by Douglas Guilfoyle

Edward Elgar Publishing Liited
ISBN: 978 1 84980 484 4

www.e-elgar.com

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



A THREE DIMENSIONAL AND ANALYTICAL LOOK AT THE MENACE OF MODERN PIRACY FROM LEGAL AND ACADEMIC VIEWPOINTS

'This book,' says editor Douglas Guilfoyle 'considers the legal challenges posed by privacy and in doing so attempts to bring together the perspectives of both public and private lawyers.' Indeed, as the publishers Edward Elgar have explained, 'Modern Piracy' is the first book to survey the law of maritime piracy, both from the perspectives of public and commercial law.

In one compact volume, it presents a wide cross section of expertise on this fraught and increasingly worrisome subject from at least a dozen learned contributors-- academics and practicing lawyers-- of which the editor is one. Hailing from a variety of backgrounds, they collectively offer the reader the benefit of a dazzling array of academic qualifications and practical, top-level experience.

As mentioned in the preface, the book reflects the work of the Modern Laws of High Seas Piracy Project, the members of which have come from academia, government and private practice, primarily in Europe, North America and South East Asia. Who better then, to offer the reader an extremely useful range of opinion and insight into the problem of piracy!

One of the aims of the book, as the editor explains, is to consider piracy 'in the round'. Piracy in context is dealt with in Part I while Part II examines the law from a state and government perspective.

In Part III the law is examined as it relates to the concerns of private business, including the legal framework and the general law of marine insurance in relation to piracy, including a range of matters pertaining to risk.

Piracy of course encompasses a wide spectrum of crimes, from violence and detention on the high seas to criminal acts within territorial or internal waters, including 'armed robbery against ships' and more besides.

In Part IV therefore, a number of conclusions are reached - at least tentatively- surrounding the various themes that are common to the fight against piracy, including concepts of efficiency, justice and law enforcement, centring on state intervention-- including the military-- as opposed to private initiatives.

The work is extensively and meticulously footnoted, with a detailed index at the back, the book functions as an excellent research tool as well as rather a riveting read for everyone from international lawyers and academics across a range of disciplines, to those specializing in maritime commercial law. Practitioners in this specialist area will certainly appreciate this current, contemporary and practical examination of it.

The publication date is cited as at 2013.

Governance of Seas and Oceans

(Oceanography and Marine Series Seas and Oceans Set)

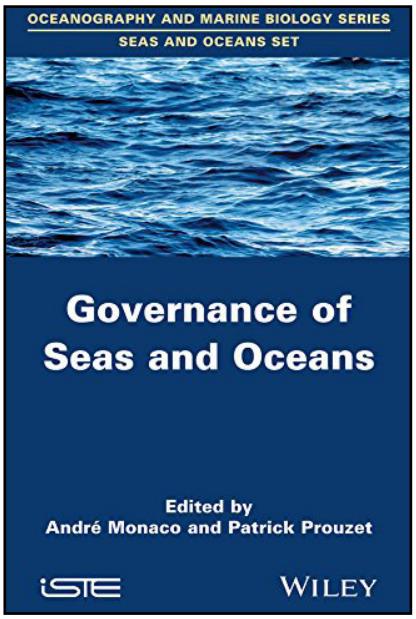
Edited by André Monaco and Patrick Prouzet

Published by Wiley-ISTE (November 2015)
ISBN: 978 1 84821 780 5

Available as an ebook

www.iste.co.uk
www.wiley.com

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



LEGAL PRINCIPLES MEET ENVIRONMENTAL SCIENCE IN THIS IMPORTANT NEW WORK OF RESEARCH

As there is more water than dry land on this planet, (comprising over 70% of the earth's surface) our seas and oceans should be considered a treasured and fundamentally vulnerable resource. Governance – enlightened and informed governance, that is – is the driver behind the decision-making processes that lead to sensible management of the marine environment.

Recently published by ISTE Ltd. and John Wiley as part of their 'Oceanography and Marine Biology Series,' this book makes an important contribution to the literature of environmental law, as part of a cross-disciplinary - and actually a holistic- approach to the conservation of marine spaces and marine resources. It contains articles from eighteen international and highly qualified contributors from universities and research institutes in France, mainly Brittany. The exception is Paul Holthus who hails from the US state of Hawaii.

With its variety of individual contributions, the book if anything, points up the close linkages and overlaps between science- particularly the environmental sciences- and the law. What you could call a symbiotic relationship between scientific and legal disciplines is demonstrated in at least four of the book's eight chapters. The titles are indicative.

The first chapter examines 'transformations' in the international law of the sea, with reference to marine spaces and marine resources, each explained in detail. Here, the Law of the Sea is pinpointed as the key to the governance of maritime 'spaces'.

Briefly described is the fascinating history of the Law of the Sea, which had its beginnings in Roman times (and no doubt long before).

Chapter 2 discusses the governance of international shipping traffic by maritime law, while Chapter 3 introduces the international law on marine pollution, particularly the pollution caused by ships-- a key area of concern. Chapter 5 explores the main legal issues emanating from marine renewable energies, for example, the legal complexities which pertain to the installation of off-shore wind turbines.

Seas and oceans (there's a difference) continue to deliver almost innumerable commercial and industrial benefits and opportunities, from transport and fishing to international tourism, with a collective value within the world economy that is almost incalculable.

It is significant that the expert contributors to this book have examined these and other aspects of the marine environment primarily from a legal point of view. The result is that oceanographic knowledge, socio-economic analysis and legal principles are brought together in one volume.

Environmental lawyers…decision makers in government bodies…and opinion formers in the media, as well as students and academics-- will find the perspectives offered in this book both enlightening and useful.

The publication date is cited as at 2015.

Sailors' Society exists to help seafarers and their families worldwide by delivering welfare, education and poverty relief.

TRANSFORMING SEAFARERS' LIVES

Sailors' Society

By becoming a corporate partner with us, you can progress towards your CSR goals – and change seafarers' lives at home, in port and at sea.

Contact Claire Heath at partnerships@sailors-society.org today to find out more.

Tel. +44 23 8051 5950
www.sailors-society.org

Registered Company No: 86942
Charity No: 237778