Dr Karen Sumser-Lupson.

ADDRESSING AFRICAN MARITIME CYBER CHALLENGES

ABSTRACT

Cyber Security is currently one of the major threats to legal maritime practices it is global, complex multi-dimensional and straddles international and national borders. International criminals that use cyber tactics have advanced technical skills and currently there are few legal frameworks that can embrace the totality of the cyber-criminal network. The cybercriminal space is no longer embryonic, it is a sophisticated network of global criminals that often collaborate and is rapidly moving towards exploiting gaps in the maritime security interface, creating a real challenge for ports and all aspects of shipping and logistic chain. This paper will examine known challenges, provide key examples of cyber-attacks within the maritime domain and critically scrutinise response mechanisms along with the current barriers restricting the sustainable application of the associated legal processes.

BACKGROUND.

The evolvement of modern technologies in particular Information Communication Technologies [ICT][1] has positively contributed to the effective streamlining of ports, shipping and logistic chain management practices. Better communications, electronic systems with seafarers often dependant on technology data more so than their own skills and knowledge. Advanced navigation computer systems and programs are used for the rapid disembarkation of passengers, loading, handling, and tracking of goods at ports. These supporting technologies are now an everyday part of the shipping and logistic structure. More importantly technologies embrace real-time cargo tracking, crew and passenger management applications, windows-based radar and floating data centres.

Considering that the maritime industry is highly competitive and demand driven it is critical that ports and associated shipping companies can optimise their costs within the international legal framework in order to maintain customer and government credibility.

BENEFITS OF ENHANCED ICT FOR PORT AND SHIPPING/LOGISTIC COMPANIES

There are two specific benefits for maritime industries to multiply their use of modern and emerging technologies.

The first need to respond to increasing demands and obligations to international convention; these are set out by the International Maritime Organisation (IMO). The IMO has six main bodies [Note2] concerned with the adoption or implementation of conventions; developments in shipping and other related industries are discussed by Member States in these bodies, and requirements for new convention or amendments to existing conventions can be raised in any of them[3].

The second is increasing company efficiency by combining leading ICT communications technology and proficiency into an end-to-end management system by improved cost control, flexibility, scalability, modularity and competitiveness; standardized processes; seamless integration between shore based and offshore IT and communications infrastructure

1 Note: Information and communication technology is a vast field encompassing virtually all technologies that can store, receive or transmit signals electronically.
2 Note:The Assembly and Council are the main organs, and the committees involved are the Maritime Safety Committee, Marine Environment Protection Committee, Legal Committee and the Facilitation Committee.
[3] International Maritime Organisation : Convention and their Application.
Http://www.imo.org/en/About/Conventions/Pages/Home.aspx Accessed 25.03.16

INTERNATIONAL CONVENTION

International Convention is the procedure from which the International Maritime Organisation [IMO] assists individual governments and the global maritime community to apply the primary International law as set out under the United Nations Committees Law of the Sea [UNCLOS]. Before a convention comes into force and becomes binding upon the Governments which have ratified it, it has to be accepted formally by individual Governments. The terms of signature, ratification, acceptance, approval and accession are the means by which a State can express its consent to be bound by a treaty.

In the main most conventions that are adopted (for which the IMO is responsible for monitoring), can be categorised under three headings.

1. Maritime safety;
2. Prevention of marine pollution; and
3. Liability and compensation, especially in relation to damage caused by pollution.

Other groupings are conventions that deal with facilitation, tonnage measurement, unlawful acts against shipping and salvage, etc[3].

Typically adopted conventions are designed to help eliminate poor practices, to address common concerns and to progress the modernity of the international maritime industry in general. Below are a few examples of relevant regulation/convention:

- Regulation 19 of SOLAS Chapter V - Carriage requirements for shipborne navigational systems and equipment - sets out navigational equipment to be carried on board ships, according to ship type. In 2000, IMO adopted a new requirement (as part of a revised new chapter V) for all ships to carry automatic identification systems (AISs) capable of providing information about the ship to other ships and to coastal authorities automatically.

- Regulation 19 of the new Chapter V - Carriage requirements for shipborne navigational systems and equipment allows an electronic chart display and information system (ECDIS)[4] to be accepted as meeting the chart carriage requirements of the regulation.

- The obligations of ships to transmit LRIT information and the rights and obligations of SOLAS Contracting Governments and of Search and rescue services to receive LRIT information are established in regulation V/19-1 of the 1974 SOLAS Convention.

- The IMO's International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), 1978. In 1995 the STCW Convention was completely revised and updated to clarify the standards of competence required and provide effective mechanisms for enforcement of its provision.

- The International Convention for the Prevention of Pollution from Ships (MARPOL) in 1973. This has changed over the last few decades to include a much wider range of measures to prevent marine pollution, and the original MARPOL Convention was amended many times to also include requirements addressing pollution from chemicals, other harmful

[4] The regulation requires all ships, irrespective of size, to carry nautical charts and nautical publications to plan and display the ship's route for the intended voyage and to plot and monitor positions throughout the voyage. But the ship must also carry back up arrangements if electronic charts are used either fully or partially.

substances, garbage, sewage and, under an Annex VI adopted in 1997, air pollution and emissions from ships.

- 1974 SOLAS Convention (chapters VI and VII and other relevant parts, as appropriate);
- MARPOL (Annexes III and V, as appropriate);
- International Convention for Safe Containers (CSC), 1972;
- International Maritime Dangerous Goods (IMDG) Code and related supplements;
- International Maritime Solid Bulk Cargoes (IMSBC) Code and related supplements;
- International Code for the Safe Carriage of Packaged Irradiated Nuclear Fuel, Plutonium and High-Level Radioactive Wastes on board Ships (INF Code);
- Code of Safe Practice for Cargo Stowage and Securing (CSS Code).

The steady increase of convention and the government obligations concerning the maritime industry has resulted in ever increasing workloads for ports, shipping and logistic companies. To manage extra workloads effectively many companies have incorporated the use of complex digital systems to sustain operations and to ensure that they can provide a total quality control management system from which to maintain due diligence and record their actions.

This leads to the second benefit which is increasing company efficiency by combining leading ICT communications technology and proficiency into an end-to-end management system by improved cost control, flexibility, scalability, modularity and competitiveness; standardized processes; seamless integration between shore based and offshore IT and communications infrastructure.

INCREASING COMPANY EFFICIENCY USING ICT SOLUTIONS

ICT is the conventional solution for unlocking, enhancing and streamlining a company's capability in the market place. Over the past two decades merchant vessels and ports have continuously increased in size and have adopted complex and more sophisticated electronic systems. Ship crews have significantly decreased in size as dependency for computer systems that can be used for navigation, as well as for rapid unloading, handling, and tracking of goods at ports have increased. Global Positioning Systems (GPS), maritime Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS) are all integral to IMO mandatory convention and are used for viewing digital nautical charts.

Vessels can be tracked from almost any geographical location on the planet as can their cargos. Ports because they provide a strategic hub within which trade is unloaded/or loaded stored or moved from one transport mode to another are also integral to the shipping logistical process and are both a central and critical infrastructure. Ports utilise a wide variety of electronic ITC systems such as Vessel Management Systems (VMS), along with customs, and other administrative practices *(see Table 1 below)*

Container shipping in particular has been one of the most rapid industry developments in this century; however it also brought with it many complications as the generation of paperwork associated with each item started to become untenable. The advocating of systems such as the 'single window[5]' approach allowed for a streamlined process within which to embed standardised documents within a single entry point and this significantly reduced the man handling of documents through a multiple system. On the back of that additional ICT support systems have developed which allow individual customers to track his/her 'item' with reference to the real time location of the unit and the estimated date of arrival.

[5] Note: Definition of single window by founder John Barnes Odonkor "A facility that allows parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfil all import, export, and transit-related regulatory requirements. If information is electronic then individual data elements should only be submitted once."

Shipping and port logistic[6] services, information systems and infrastructure/resources are in fact three closely linked components and contain the following:

- Logistics services; support the movement of materials and products from inputs through production to consumers, as well as associated waste disposal and reverse flows. They include activities undertaken in-house by the users of the services (e.g. storage or inventory control at a manufacturer's plant) and the operations of external service providers. (e.g. transport, storage) as well as non-physical activities (e.g. supply chain design, selection of contractors, freightage negotiations). Most activities of logistics services are bi-direction.
- Information systems; include modelling and management of decision making, and more important issues are tracking and tracing. It provides essential data and consultation in each step of the interaction among logistics services and the target stations.
- Infrastructure; comprises human resources, financial resources, packaging materials, warehouses, transport and communications. Most fixed capital is for building those infrastructures[7].

Categories of Organizational Performance Found in Literature		
Category of organizational performance	**Performance indicators**	**Sources [Inc. General Studies]**
Financial performance/Firm performance	profit, ROI, ROA, return on sale, profitability, cash flow, profit-to-revenue ratio	Evans (2007), González-Benito (2007), Feng et al. (2008), Green et al. (2008)
Market performance/Marketing performance/Commercial performance	market share, market growth, sales volume, sales growth, market development, new product/service development, competitive position, reputation and image, access to global market;	Studies on SC and maritime security Williams (2008) Evans (2007); González-Benito (2007); Feng et al. (2008); Green et al. (2008).
Operational performance/ Manufacturing performance/ Internal business performance/ Supply chain performance/ Logistics performance/Quality outcomes	quality (service, product), cost, productivity, flexibility, reliability (dependability), visibility, delivery speed, transit time, delivery failure, employee turnover, efficiency, response time, defect rate, variety of service, shipment accuracy, internal procedures, employee morale, resilience, safety, risk, security.	Feng et al. (2008); Green et al. (2008).
Customer performance	customer relationship, customer satisfaction, number of customer contact points, customer retention rate, customer commitment, knowledge of customers' needs	Evans (2007).

TABLE 1. EXAMPLES OF WHERE THE USE OF IT SOLUTIONS TO INCREASE COMPANY EFFICIENCY

KEY ICT TRAITS

- Volume: By 2035, the volume of information received by a single ship will virtually be unlimited, leading to a potential overflow of information.
- Quality: The quality or accuracy of the information matters more than the quantity.

[6] NOTE: Council of Logistics Management (1991) defined that logistics is 'part of the supply chain process that plans, implements, and controls the efficient, effective forward and reverse flow and storage of goods, services, and related information between the point of origin and the point of consumption in order to meet customers' requirements'.

[7] Proceedings of the Eastern Asia Society for Transportation Studies, Vol. 5, pp. 1657 - 1672, 2005: The Role of Transportation in the Logistics Chain.

- Distribution: The tendency is towards a P2P rather than hierarchical distribution of information; every platform is a sensor within the global grid and every platform is networked.
- Trustworthiness: Information must be trusted, which is getting more difficult in an environment where operations are mainly conducted jointly with partners, increasing the risk of a weaker link within the network[8].

TRENDS

Complexity of Information Management: Complex and non-hierarchical networks of information sharing, the increased speed of communication, the increasing number of information providers, sources and end-users involved in the process, all contribute to the complexity of information management. Processing the volume of information, making sense of the complex flow of data, transforming information into intelligence engenders a complex information management structure.

Information Breach: Communication being mainly dependent on IP-based systems, there is an increased risk of information breach. Information can be accessed, usurped or corrupted. The complexity of the networks and the multilateral and joint operating environment also contribute to increasing the risk of information breach.

Considering increasing global expectations maritime industries are compelled to embrace new technology such as ICT systems if they are to stay on top of their international obligations and to remain commercially competitive and viable. However modern technologies are very vulnerable to cyber threat. Cyber challenges are currently identified as the emerging maritime security plague and in as much as the technology is resolving issues it conversely is generating new challenges. Kate Kochetkova in May 2015 reported that the 'Maritime industry is easy meat for cyber criminals'. The maritime and offshore sector is in fact singled out as being particularly vulnerable to hacker attacks and this is aggravated due to its size and diversity.

MARITIME CYBER CHALLENGES

Cyber challenges have been rapidly escalating over the past decade and probably the most well-known international cyber 'criminals' are Anonymous.

This particular group extend their global reach through a network of individual 'hackers' *(See NOTE*[9]) and group 'hacktivists' which have pledged their allegiance to Anonymous and their mandate. In Dec 2011the group announced that they had carried out Operation 'Robin Hood' an attack on the American security firm Stratfor, a Texas-based company which produces analysis on international security issues for international clients including banks, oil companies and police agencies.

As well as claiming to have donated $500,000 to charities online using the stolen data, the hackers posted parts of their haul online. The files included more than 50,000 credit card numbers of which 10,000 were not expired, 87,000 email addresses and 44,000 encrypted passwords, of which around half could be easily cracked. Major British firms such as BP, HSBC and Tesco were also named in the files[10].

[8] Mr Oliver Fitton, et al., (2015) Cyber Opportunities in the Maritime Space. Lancaster University. http://eprints.lancs.ac.uk/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf

[9] NOTE: Hacker, in its original sense, described someone who used or adapted a technology for a purpose it was not originally intended in a way it was not designed.

[10] Christopher Williams, Technology Correspondent. 28.12.11 http://www.telegraph.co.uk/technology/news/8980453/Anonymous-Robin-Hood-hacking-attack-hits-major-firms.html Accessed 28th March 2016

Anonymous are extremely confident in their cyber-attack operations using a YouTube video station to promote their activism and operations. Anonymous cyber-attack operations have been launched from many countries including the US, UK, Australia, the Netherlands, Spain, and Turkey. The group have been recognised as "freedom fighters" or digital Robin Hoods while conversely they are described as "a cyber lynch-mob" or "cyber terrorists".[11] Anonymous attacks have been made on the Islamic State or ISIS, corporations such as PayPal, MasterCard, Visa, and Sony and Nations in particular Israel.

Looking specifically at maritime the complexity of ICT systems have provided plentiful opportunities for cyber criminals to exploit. In particular are the security gaps in the principal vessel technologies such GPS, Automatic Identification System (AIS) and the Electronic Chart Display and Information System (ECDIS).

For example should there be a breach in GPS system a ship could be 'pirate ghosted', which means it can be manipulated remotely, without the Masters knowledge and send a ship off-course while making her appear to be on-course. Pirates could take full advantage of this capability and wait for the ship to come to them rather than chase down a vessel. Pirate ghosting could also cause for collisions, groundings and delay trade delivery.

Cyberkeel[12] reported in 2014 that during 2010 as a result of the vessels computers and control systems being riddled with viruses, a drilling rig was tilted from its construction site in South Korea towards South America. Remediation of the hack took 19 days.

Business disruption; during august 2011, hackers penetrated the servers of IRISL, Iranian Shipping Line, damaging data with rates, loading, cargo numbers, delivery dates and places. Nobody could specify the location of certain containers. A considerable amount of cargo was delivered to the wrong destinations or even lost[10]. As a fact by breaking into key container terminals it is possible for criminals to aggressively disrupt regional and national supply chains operations, which could result in significant repercussions for a government. For example Cyberkeel documented that the British government publicised that discovered cyber-attacks had cost the UK oil and gas industry about 400 million pounds ($672 million) in a single year; this did not consider those undiscovered.

Piracy: Somali pirates employed hackers to infiltrate a shipping company's cyber systems to identify vessels passing through the Gulf of Aden with valuable cargoes and minimal on-board security which led to the hijacking of at least one vessel.

Drug Crime and Smuggling, in 2011 the Port of Antwerp was attacked by cyber criminals; (identified as an attack organized by a drug cartel) they successful assaulted and gained control over the ports terminal systems. The group were able to release containers to their own truckers without knowledge of the port authorities and then removed information about contraband containers from all databases. It was some two years later in late 2013 that the hack was finally discovered and the problem fixed.

In 2012 hackers, working for a criminal syndicate, compromised the cargo system controlled by the Australian Customs and Border Protection Service agency. Cyber criminals wanted to know which shipping containers were suspected by the police or customs authorities. With this data they'd know if they needed to abandon particular containers with contraband cargo[10].

Terrorist activities; multimodal, kinetic and non-kinetic threats to international peace and security, includes cyber-attacks, low intensity asymmetric conflict scenarios, global terrorism, piracy, transnational organized crime, resources security, retrenchment from globalization and the

11 Rawlinson, Kevin; Peachey, Paul (April 13, 2012). "Hackers step up war on security services". The Independent. – via HighBeam Research (subscription required). Accessed March 2016

12 Cyberkeel (2014) Maritime Cyber Risks. Copenhagen, Denmark. http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf

proliferation of weapons of mass destruction, are identified by NATO as 'hybrid threats,' [13] NATO also underlined that hybrid threats were so new that state actors are ill-equipped to handle[14].

The maritime domain and activities that occur there are very much on the radar of known terrorist groups such as Daesh (ISIS-ISIL). It was reported by Reuters in Jan 2016[15] by the chief of NATO's Allied Maritime Command, Vice-Admiral Clive Johnstone; that Daesh militants want to 'build their own maritime force to carry out terror attacks on cruise or commercial ships in the Mediterranean Sea using sophisticated sea-based weapons' and that the known terrorist group is 'striving to mount seaborne operations, endangering commercial and passenger sea lanes'.

The use of cyber-attack as a form of warfare is also not unusual; the US, for example openly state that they use network-based electronic attacks such as radio jamming or electronic sabotage as an integrated part of their military operations. During March 2016, the US Defence Secretary Ashton Carter[16] stated that ongoing cyber-attacks were intended to "interrupt and… disrupt ISIL's command and control, to cause them to lose confidence in their networks, to overload their networks so they can't function, and to do all of these things that will interrupt their ability to command and control forces there, control the population and the economy."

If one considers that these types of operations could also be used could also be used by an aggressive organisation to plan an intervention and boarding of a vessels transiting sea lanes or to disrupt port activities and the flow of commercial trade. The fact that piracy, driven by financial reward caused for major impacts to the shipping industry and the global economy; it is not difficult to visualise the array of cyber disruptive opportunities available to terrorist groups and the potential global economic outcomes.

CYBER-ATTACK MAGNIFIERS

One of the fundamental problems of dealing with a cyber-attack is that cyber criminals tend to be particularly clandestine and are very good at covering up their tracks, in doing so companies are often unaware they have been hacked; as was the case of the port of Antwerp. Additionally once hackers have accessed a system, they can control it remotely, try and outwit any attempt of being identified, or worse, lay a trap that could set off a serious of events (commonly known as a worm) to erase or invalidate complete data files if discovered.

Another issue is that the sophistication and technological expertise of criminals operating within the cybercrime sphere is high and if a situation occurs on a ship where systems are compromised, it is unlikely that any member of a ship's crew would have the necessary expertise to 'fix' the problem. Such a situation was reported by Reuters[17] in 2014 whereon a hacked floating oil rig had to shut down for a week before the issue was cleared out because there were no cyber security professionals onboard.

13 Dr. Sascha-Dominik Bachmann and Dr. Håkan Gunneriusson [2014) Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive Approach. The Journal on Terrorism and Security Analysis. JTSA

14 Assessing Emerging Security Challenges in the Globalized Environment," NATO Allied Command Transformation, https://transnet.act.nato.int/WISE/CHTIPT/Newsletter/JanuaryCHT/file/_WFS/CHT%20 Newsletter%20-%20Edition%201%20-%20final.pdf.

15 Reuters 29th Jan 2016: Article ISIS wants own sea power to carry out attacks in Mediterranean, NATO naval chief warns. https://www.rt.com/news/330569-isis-naval-arm-mediterranean/ Accessed 23.03.16

16 Sean Gallagher (US) - Mar 1, 2016 7:07pm GMT. US military launches cyber-attacks on ISIS in Mosul, and announces it. http://arstechnica.co.uk/information-technology/2016/03/us-military-launches-cyber-attacks-on-isis-in-mosul-and-announces-it/ Accessed 25.03.16

17 Reuters: (2014) All at sea: global shipping fleet exposed to hacking threat SINGAPORE | By Jeremy Wagstaff. http://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424

Frustrating the situation is the fact that often hacked victims try to keep successful hacks a secret. This is because maritime companies value their reputation more than the money they actually lose even though each hack can cost millions of dollars to ship owners or ports.

How can the Maritime Sector Respond to Cyber Challenges?

In 2014 and because of the dramatic increases in the use of cyber systems across the maritime sector and related risks Canada[18] provided a paper to the International Maritime Organisation which proposed the development of guidelines on maritime cybersecurity. The paper suggested that cybersecurity guidelines needed to be developed specifically for the maritime sector and these could help protect ports, terminals, vessels and other stakeholders, as well as help mitigate the effects of successful intrusions and prevent disruptions to international trade, by providing guidance on areas of cybersecurity. The justification for the proposed guidance materials was based on the exponential growth of maritime stakeholders use and reliance on cyber systems and that a successful cyber-attack against a maritime stakeholder could have significant negative effects on the global economy and disrupt international trade.

The suggested Cyber Security Guidelines included the following:

1. A description of types of cyber systems typically used by maritime sector stakeholders to support their operations;
2. A description of potential cybersecurity vulnerabilities associated with the types of cyber systems typically used by maritime sector stakeholders;
3. A description of mitigations that could be implemented by maritime sector stakeholders to address potential cybersecurity vulnerabilities.

The proposed voluntary maritime cybersecurity guidelines would:

a) Be consistent to the greatest extent possible with similar cybersecurity guidelines previously promulgated by international organizations, such as the International Organization for Standardization;
b) Identify implementable measures to enhance cyber security, but not include specific technical requirements or recommendations to use specific hardware, software, policies or processes.
c) Canada could provide to correspondence group members' results of research conducted as part of the development of a Maritime Cybersecurity Strategic Framework, including information on cyber systems used in the maritime sector and associated potential vulnerabilities and mitigations, to serve as a basis for discussion.

The also paper outlined the following five categories to illustrate to maritime sector stakeholders the rationale and importance of identified vulnerabilities and mitigations, categories which could be adopted or adapted by the proposed correspondence group; they are:

1) access control – ensuring sensitive data and hardware are accessed or altered only for legitimate ends;
2) network design – taking a holistic and risk-based approach to implement security measures that balance between accessibility and security for different systems, data, and other network components;
3) intrusion detection – putting in place measures to detect intrusions by malicious actors and limit ongoing harm;

[18] IMO (2014) Ensuring Security in and Facilitating International Trade: Measures toward enhancing maritime cybersecurity. http://www.protect-group.org/assets/Uploads/FAL-39-7-Measures-toward-enhancing-maritime-cybersecurity-Canada.pdf. Accessed 23/03/16

4) communication security – ensuring information communicated within or outside an organization is received by the person for whom it was intended without alteration; and,
5) governance – establishing a management framework, including strategic planning, employee engagement and specific policies, to align resources and behaviours with an organization's cybersecurity needs.

LEGAL IMPLICATIONS

However, these guidelines do not cover the complexity of legal implications for the cyber domain, lawyers who work within the maritime sector or on national defence issues. In the future these lawyers will be significantly challenged to rethink long-held ideas of international law[19].

For example, with regards to a terrorist cyber threat. The extensiveness of civilian involvement in the cyber domain, both inside and outside of government, will place even greater stress on traditional notions of legitimate participation in armed conflict. One of the realities of the cyber domain is that 'combatants' in international armed conflict and security personnel in internal ones cannot defend all the national digital assets on their own. Assets such as maritime critical infrastructure and the threats posed to them, are too numerous and broadly distributed.

Cyber activity represents a true expansion of the "home front" as an area of operations, even into the boardrooms and bedrooms of nations. As a result, many participants in cyber asymmetric operations are unlikely to be wearing uniforms or bearing arms.

The legal point considers that being in compliance with the requirements of domestic law in what they are undertaking, they are thus not illegitimate under international law. Nor should they be liable to foreign prosecution for doing so. This transformative nature of cyber is reflected in the example of an individual who was passing on details regarding fuel tankers at a Libyan port and who was eventually identified to be a forty-eight-year-old ice cream business supervisor in Arizona. This leads to the following question; is a person who takes information posted by someone else from the web and passes it on taking a direct part in hostilities?

Interpretive guidance makes a link between the transmittal of 'tactical intelligence' and the 'potential causation of harm' resulting from any targeting decision. However these also raise questions of degrees of remoteness and where the line can be drawn with cyber challenges.

The multi-dimensional aspects of the cyber challenge are so profound that international lawyers are also going to have to be prepared to understand and explain why combatant status will matter when assessing a cyber-attack that has a global reach but tangible domestic impact. This means that some military lawyers, whose area of expertise may be limited to the law of armed conflict, will need to become much better acquainted with the impact jus ad bellum, international human rights law and domestic law have on cyber operations; whilst civilian lawyers will need to understand at what point the line has been crossed and a perpetrator of a cyber-attack should be considered within the realms of 'law of armed conflict'.

From a legal perspective the following must be considered is cyber-crime like theft, vandalism, fraud and kidnap, but perpetrated in "cyberspace", using computer code over the internet? How is it different from conventional crime? The greater distance and time between the criminal and the crime? The scale of the proceeds of the crime in terms of volume and value? And. . the manner in which the consequences can cascade across enterprises and market sectors? *ENISA (2011)*

[19] Cabinet Office, (2011)The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World, available at http://www.Cabinetoffice.Gov.Uk/Sites/Default/Files/Resources/Uk-Cyber-Security-Strategy-Final.Pdf [Hereinafter UK Cyber Security Strategy]

One of key challenges for legal regimes therefore will be a major intensification of educational, training and doctrinal challenge for military and civilian government legal advisors.

Additionally from the maritime industries perspective the question remains how can we protect ourselves should a cyber-attack occur? Cowie, T[20] (2015) representing Swiss REA in response to the question 'Is Cyber covered under a Marine Insurance Policy? . . . stated that 'Marine Insurance Policies are so varied and/or bespoke, it is hard to give a definite answer, but assuming an "all risk policy" without a proper exclusion, then I would say yes, cover would be found for a "Cyber" loss.

CONCLUSIONS AND RECOMMENDATIONS ADAPTED FROM *[ENISA, 2011]* [21]

The awareness on cyber security needs and challenges in the maritime sector is currently low to non-existent. African Member States should consider developing and implementing awareness raising campaigns targeting the maritime actors. In particular the provision of appropriate cyber security training to relevant stakeholders (e.g. shipping companies, port authorities, etc.) is highly recommended. Such awareness campaigns and training initiatives should target all relevant actors involved in the maritime sector, while their provision could be coordinated by relevant cyber and maritime competent organisations (e.g. national cyber security offices, public-private partnerships, etc).

ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR

Due to the ranging ICT complexity and the use of specific technologies, there are particular challenges to ensure adequate security provisions in maritime systems. It would be beneficial for all stakeholders to agree on 'a common strategy' and 'development of good practices' for the technology development and implementation of ICT systems in the maritime sector and ensuring "security by design" for all critical maritime ICT components.

As current maritime regulations and policies consider only the physical aspects of security and safety, it is recommended that policy makers add cyber security aspects to them.

It is strongly recommend a holistic risk-based approach, which would require the assessment of existing cyber risks associated with the current ICT systems implementations relevant to the African maritime sector as well as the identification of all operational associated critical assets. For maritime economic operators and stakeholders, it is important to proactively apply sound cyber and information security risk management principles within their organisations and environments.

With the maritime governance context being fragmented between different levels (i.e. international, African, national), the International Maritime Organisation together with the African Union, AMSSA and the Member States should consider aligning and harmonizing international and African policies related to this sector, particularly on its cybersecurity aspects. Member States should clearly specify the roles and responsibilities that should be endorsed for addressing cyber security matters at those various levels.

Proper coordination and cooperation between the relevant stakeholders should also be defined (e.g. port authorities, shipping companies, etc.) through public-private sector interaction. It is recommended that Member States stimulate dialogue and public-private partnerships between the key stakeholders in the maritime sector (e.g. agencies, shipping companies, port authorities, etc.) and connected stakeholders (e.g. insurance companies / brokers).

---

[20] Cowie, T. (2015) Maritime Insurance Cyber Security – Framing the Exposure– May 2015. Swiss REA.

[21] ENISA (2011) report analysis of cyber security aspects in the maritime sector. P.O. Box 1309, 71001 Heraklion, Greece

From a different perspective, better information exchange and statistics on cyber security may help insurers to improve their actuarial models, reduce own risks, and therefore offering better contractual insurance conditions to the involved maritime stakeholders. Information exchange platforms, should be also considered and developed by Member States in order to foster and facilitate communication on cyber security for the relevant maritime actors.

Hybrid threats as such are not new threats; new is the recognition that such multimodal threats command a 'holistic' approach, which combines traditional and non-traditional responses by state and non-state actors such as multinational corporations. Responses to hybrid threats must be proportionate and measured: from civil defence and police responses to COIN and the use of military force. Hybrid threats pose not only maritime security challenges but also legal difficulties it is critical that Member States through military doctrinal reform, adapt within their existing legal and operational frameworks.

Finding	**Recommendations**	**Time line**
Low awareness and focus on maritime cyber security	Design and launch awareness raising campaigns Develop appropriate trainings	Short term Mid term
Complexity of the maritime ICT environment	Build strategies and good practices defining security requirements for ICT implementations in the maritime sector.	Short term
Fragmented maritime governance context	International level: help align and harmonize international and African policies on maritime cyber security requirements;	Long term
	African level: define clear roles and responsibilities for addressing cyber security matters in the maritime sector;	Mid term
	National/regional level: enforce African standards (develop standards and enforce rules in the core text) for ports requirements on ICT systems.	Long term
Inadequate consideration of cyber security in maritime regulation	Take appropriate measures in order to add considerations towards cyber security in the regulatory frameworks governing the maritime sector.	Mid term
Absence of a holistic approach to maritime cyber risks	Define and implement a holistic, risk-based approach to address the subject of maritime cyber security.	Mid term
Overall lack of direct economic incentives to implement good cyber security in the maritime sector	Stimulate dialogue and information exchange between key stakeholders in the maritime sector and connected stakeholders (e.g. insurance brokers).	Short term
Inspiring initiatives	Establish information exchange platforms based on trust-based public-private partnerships.	Long term
Civilian/Military Cooperation	Establish information exchange platforms based on trust-based Civ/Mil cooperation. E.g. Maritime domain / Situational awareness.	Long term

African Maritime Safety and Security Agency (adopted from ENISA (2011)

END: