COMMENTS ON THE PAPER TITLED: ADDRESSING AFRICAN MARITIME CYBER CHALLENGES

BY CHINWE NDUBEZE

AT THE 14TH INTERNATIONAL MARITIME SEMINAR FOR JUDGES

ON 31ST MAY – 1ST JUNE 2016

AT SHERATON HOTEL AND TOWERS, ABUJA

INTRODUCTION

- The advent of the internet brought in its wake ease and convenience in electronic communication. Various aspects of daily lifeare now dependent on Information Communication Technologies (ICT) like, banking. Business, paying bills, shopping, relationships etc.

- The growth of mobile communication and convergence of technologies(the combination of two or more different technologies in a single device, e.g. taking pictures with a cell phone, browsing the web on a television etc.) is now our present day reality.

- There also appears to be the need to prepare for the anticipated growth of "Internet of Things" (IOT), which is being suggested by many as the 4th Revolution.

- Clearly Information Communication Technologies (ICT) has advanced and is still advancing in our time.

- Indeed life is getting smarter but are we getting any smarter in the way we protect ourselves on these platforms?

- Notably, effective use of ICT requires imputing one form of data or the order.

- Accordingly, it has become imperative to protect sensitive data and information communication systems to ensure their functionality, optimal performance and also to avoid vulnerabilities.

- Unsurprisingly, the maritime industry is becoming increasingly dependent on ICT and the use of data.

- Dr karen Sumser-Lupton, noted in the Paper under review that this growth has positively affected the entire maritime industry.

- This fact also has advantages relating to safety, efficiency and profitability.

- Haugland, B. K (2014)[1], also posited that ICT will make shipping safer, smarter and greener.

- So how true is this assertion in the light of the various cyber threats and challenges which the African maritime sector is confronted with? And can these challenges be effectively addressed?

[1] Haugland, B. K (2014). ICT will make shipping Safer, Smarter and Greener http://blogs.dnvgl.com/sustainability/2014/03/ict-will-make-shipping-safer-smarter-greener/

ISSUES RAISED

- Our comments will be hinged on the salient and troubling issues raised by the Paper of Dr karen Sumser-Lupton regarding addressing the African Maritime Cyber Challenges. They include:
- Reality of Cyber Threats
- Challenges in combating the threats
- Key examples of cyber attacks
- Response mechanisms
- Current barriers restricting the sustainable application of the associated legal processes

IS THE THREAT REAL?

- [2]IBM's 2015 Cyber Security Intelligence Index suggests that the majority of adverse cyber incidents happen within the finance and insurance, manufacturing, and information and communication industries, rather than in the shipping or logistics sector. This may be partly explained by the fact that maritime industries have been slower to embrace the use of technology and also that the business is rather 'invisible' to the general public due to the fact that insufficient information is known about how the industry works for many hackers or criminals to invest their time. There are simpler and more rewarding targets it would appear.
- Notwithstanding, many players and researchers in the industry are in agreement with the view expressed by this Paper that there are associated risks or cyber threat brought on by the dependence of the maritime sector on ICT.
- [3]A Reuters report of 2014 described the shipping industry as 'the next hacker's playground'.

[2] Brasington, H., hadwin, S. (2015). Cyber risks and the maritime industries: risk identification, mitigation and response. Online @ http://www.nortonrosefulbright.com/knowledge/publications/137942/cyber-risks-and-the-maritime-industries-risk-identification-mitigation-and-responseAccessed 16/05/2016

[3] Brasington, H., hadwin, S. (2015). Cyber risks and the maritime industries: risk identification, mitigation and response. Online @ http://www.nortonrosefulbright.com/knowledge/publications/137942/cyber-risks-and-the-maritime-industries-risk-identification-mitigation-and-response Accessed 12/05/2016

- [4]Kaspersky report of 22nd May 2015 is also very emphatic in stating that the maritime industry is easy meat for cyber criminals.

- [5]Paganini, P. (2015) has opined that modern maritime ships are considered a privileged target for hackers and pirates that are increasing their pressure on the Maritime Shipping Industry**.**

WHO POSE THESE THREATS?

- According to the Guidelines on Cyber Security Aboard Ships(2016),[6]the following groups of individuals pose cyber threats in the maritime industry:

- **Hactivists**–whose activities can damage reputation of players in the maritime sector as well as disrupt their operations with the objective of destroying data, publication of data (e.g. Panama Papers, activities of :"anonymous") and gaining media attention

- **Criminals** -- on the other hand may be lured by financial gain and commercial and industrial espionage to sell and ransom stolen data and system operability as well as arrange fraudulent transportation of cargo

- **Opportunist** --may also be baited by the challenge of getting through cyber security defences and may further seek to earn financial gain.

- **States and state sponsored organisation** may be involved in cyber terrorism activities aimed at cyber espionage and disruption to economies and critical national infrastructure.

WHAT IS THREATENED?

- Cyber threats in the maritime industry can be divided into three types[7] namely threats to:

- Ships and safe navigation

- Ports

[4] Kaspersky report of 22nd May 2015, Maritime Industry is Easy Meat for Cyber Criminals. Online @ https://blog.kaspersky.com/maritime-cyber-security/8796/Accessed 17/05/2016

[5] Paganini, P. (2015) , Hacking Ship: Maritime Shipping Industry at Risk. Online @ http://securityaffairs.co/wordpress/35504/hacking/hacking-maritime-shipping-industry.html Accessed 17/05/2016

[6] Guidelines on Cyber Security Aboard Ships, (2016)http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=12 Accessed 20/05/2016

[7] Tzah, L. (2015). Managing the Risk to the Global Shipping Industry Part 1. Online @ http://cytegic.com/managing-cyber-risk-global-shipping-industry-part/

- Cargo handling systems and cargo and terminal operation systems
- Data (gaining access to sensitive data for financial gain and for terrorist activities including transporting drugs, hazardous materials or weapons.

Ships and safe navigation

- As noted in the Paper, there is the increased use of computerized systems for ship navigation, however, these systems are vulnerable to attacks.
- [8]Researchers at the Trend Macro Security Firm have shown that The Automated Identification System (AIS) can be broken into and real time data can also be altered. This can be exploited for criminal, social, religious or political purposes.
- [9]An additional vulnerability was detected by NCC GROUP pertaining to Electronic Chart Display systems (ECDIS) which can lead to sever disturbances in the ships' navigation.
- Ultimately, ECDIS compromise could lead to financial loss, loss of life, environmental pollution.
- When attackers gain unauthorised access, they can have the capacity to interact with the shipboard network and everything to which it is connected, sensor data can be subverted and misrepresented to ECDIS. This could influence the decision-making process of navigation personnel, and possibly lead to collision or the ship running aground. .

Ports

- Ports are critical national infrastructure and so have the potential to be lucrative targets to terrorists and hacktivists.
- Port of Antwerp attack is a key example. In 2011drug smugglers attacked the Belgian Port of Antwerp logistics system,hiding drugs inside legitimate shipments of other goods from South America, then stealing the release codes from the computer system in order to pick up the container before its real owner turned up at the port. When this proved impossible to pull off, the criminals simply hijacked the trucks carrying the containers after they left the port.

[8] Tzah, L. (2015). Managing the Risk to the Global Shipping Industry Part 1. Online @ http://cytegic.com/managing-cyber-risk-global-shipping-industry-part/

[9] Dyryavyy y. (2014) "Preparing for Cyber Battleships – Electronic Chart Display and Information System Security," Online @ https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf

Cargo handling systems, cargo and terminal operation systems

- According to Robert L. Report in eWEEK (2014)[10], in July 2014 the security company TrapX exposed The Zombie Zero campaign: a supply-chain attack targeted at robotics manufacturers as well as shipping and logistics firms, compromising systems for more than a year. Malware was pre-installed on handheld scanners and software at a Chinese supplier's factory, and then sent to seven shipping and logistics firms and one manufacturing company, in order to infiltrate their corporate ERP servers and steal financial data. The "highly sophisticated" malware was embedded in the Windows XP operating system installed on the scanner and also on the Chinese manufacturer's support website. TrapX said the handheld scanner in question is used by "many shipping and logistic companies around the world" to check items being loaded on and off vehicles such as ships, trucks or planes. So they could modify the shipping data base and could make packages appear and disappear.

ARE THERE CHALLENGES IN COMBATING THREATS?

- The Paper posited that 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 as GPS, Automatic Identification System (AIS) and the Electronic Chart Display and Information System (ECDIS). Kaspersky report of 22nd May 2015[11] is in agreement with this position that there exist vulnerabilities in software system which can be exploited by cyber criminals.

- The ease and cost of committing the crime. [12]In July 2013, it was reported that a team of researchers from the University of Texas used GPS equipment that cost only US$3,000 to take control of the navigation system of a large ship in the Mediterranean.

- Anonymity offered by the internet making it easy for criminals to cover their tracks.

- Sophistication and expertise of cyber criminals versus that of the members of ship crew.

- Reporting challenges also exists such as:

[10] Robert L. (2014). "'Zombie Zero' Cyber-Attacks Hit Logistics, Robotic Firms for Months". Online @ http://www.eweek.com/security/zombie-zero-cyber-attacks-hit-logistics-robotic-firms-for-months.html

[11] ibid

[12] Tzah, L. (2015). Managing the Risk to the Global Shipping Industry Part 1. Online @ http://cytegic.com/managing-cyber-risk-global-shipping-industry-part/

- a. Victims want to keep the attack secret to avoid announcing their vulnerability to other criminals as well as being seen as unsafe by their customers. However Data Protection Law exist in most jurisdictions that places a burden on data processors and handlers to disclose data breaches or face legal sanctions. The Nigerian Data Protection Bill is yet to be passed,
- b. Some victims are unaware of the attack like the Port of Antwerp attack incidence.
- Low awareness of cyber security needs.
- The number of targets could be unlimited, and may include governments and public utilities, such as transport systems.
- No need to overcome physical security barriers and security personnel.
- The inability of the attacker to see the direct impact of the attack on the victim can weaken psychological impact.

HOW SHOULD THE AFRICAN MARITIME SECTOR ADDRESS THESE THREATS?

- The Paper outlinedthe Guidelines provided by Canada[13] to the International Maritime Organisation (IMO) which proposed the development of guidelines on maritime cyber security relating to:
- (i). Access control – ensuring sensitive data and hardware are accessed or altered only for legitimate ends;
- (ii) 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;
- (iii) Intrusion detection – putting in place measures to detect intrusions by malicious actors and limit on-going harm;
- (iv) Communication security – ensuring information communicated within or outside an organization is received by the person for whom it was intended without alteration; and,
- (v) Governance – establishing a management framework, including strategic planning, employee engagement and specific policies, to align resources and behaviours with an organization's cyber security needs.

[13] 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 20/05/16

- Notwithstanding these recommendations, the Paper recognizes that guidelines do not cover the complexity of legal implications for the cyber domain, which lawyers who work within the maritime sector have to contend with as well as national defence issues.

RECOMMENDATION AND CONCLUSION

- The Paper made valid and legitimate short term and long term recommendations that would help the African Maritime Sector deal with cyber threats.
- However, the IBM Report of 2016 reveals that 60% of cyber-attacks in 2015 were carried out by insiders,[14] either ones with malicious intent or those who served as inadvertent actors. In other words, they were instigated by people you'd be likely to trust.
- Norton Rose Fulbright Report of March 2016[15] identifies human error, poor cyber-hygiene (e.g. a lack of encryption of devices), and poor risk awareness (e.g. an inability to spot a phishing scam) as some of the causes of cyber challenges in the maritime sector.
- Notably, information systems are only as good as the people who use them, and attacks can be either deliberate or accidental. The level of Cyber Risk posed by employees is significant and control measures need to be put in place.
- As noted by Fitton, O., Prince, D. Germond, B, and Dr Mark Lacy, M. in the Report [16]The Future of Maritime Cyber Security, "…systems are operated by people and they represent a vulnerability which cannot be patched, corrected or rewritten as they are susceptible to manipulation and are highly fallible. They are also capable of free and critical thoughts which might lead them to breach security procedures or break the law in the name of their cause."

[14] IBM 2016 Report: "A Survey of The Cyber Security Landscape" Online @ http://public.dhe.ibm.com/common/ssi/ecm/se/en/sej03320usen/SEJ03320USEN.PDF

[15]Norton Rose Fulbright (March 2016). Cyber risks and the maritime industries: risk identification, mitigation and response.
http://www.nortonrosefulbright.com/knowledge/publications/137942/cyber-risks-and-the-maritime-industries-risk-identification-mitigation-and-response Accessed 20/05/2015

[16]Fitton, O,. Prince, D., Germond, B., and Lacy, M. The Future of Maritime cyber security. Online @ http://eprints.lancs.ac.uk/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf Accessed 17/06/2026

- BancroftC. (2014)[17]made recommendations regarding protecting against insider threats which include:

- The education of staff about the need for IT and information security.

- Development of guidelines for the use of email and safe custody of sensitive information.

- Establishment of clear guidelines on the custody of key information

- The Integration of elements of both physical and logic security to protect data.

- The Security of the supply chain.

- Continuous digital monitoring

- Synergy with partnersknowledgeable in the risk landscape.

- Integration of data security/cyber risk with cyber policies and breach response and preparedness plans.

- Active involvement with local law enforcement.

- It is now clear that the maritime industry is at risk of cyber-attack and the need to be ready to mitigate those risks has become pressing indeed. Adoption of the recommendations in the Paper will position the African Maritime Industry in a better light to handle the inherent challenges of the digital age.

- Thank you for your time!!!!!

[17] Bancroftt C. (2014) "Cybercrime and the Shipping Industry" Online @ http://www.sfmx.org/support/amsc/cybersecurity/webdocs/Cyber%20Fraud%2010-2014.pdf Accessed 22/05/2016