Towards cyber security readiness in the Maritime industry: A knowledge-based approach

Authors: **Dr Alexeis Garcia-Perez**
Dr Mick Thurlbeck
Eddie How

Synopsis:

Cyber security refers to the ability to prepare for, react to and recover from incidents (i.e. attacks) initiated from an Internet-connected device against other devices or the information they contain. Recent developments in the cyber security field show an increasing number of industries becoming targets of cyber attacks. With vessels, terminals, ports and transport operators relying on increasingly integrated and interconnected information systems, the maritime industry is no exception. Incidents have already been reported where unauthorised or accidental access to systems (e.g. a vessel's Automatic Identification System, AIS) have resulted in failure of critical systems with potentially catastrophic consequences including loss of life, environmental damage and revenue loss. Despite having a technical dimension, there is consensus in the fact that cyber security is no longer a technology issue. Cyber security affects and is affected by the industry's internal aspects, functions and processes, as well as a wide range of factors including economic, environmental, legal and political issues to name a few. Local, national and international factors also become essential when implementing cyber security management strategy and driving people's behaviour towards cyber security in the maritime industry. This paper will outline some of the major cyber security challenges faced by the maritime industry. It will then provide an overview of the key dimensions of a cyber security management strategy that could help the maritime industry learn from other sectors in the definition of a long-term, dynamic cyber security management strategy with focus on their people, processes and technology.

Bio's:

Dr Alexeis Garcia-Perez is a Reader in Cyber Security Management at the Centre for Business in Society. A PhD in Information Systems and Knowledge Management from Cranfield University complemented his original background in computer science. With a socio-technical understanding of information systems Alexeis has focused over the last decade on the wider challenges of data, information and knowledge management in organisations and society. He collaborates extensively with key players from industry and with the public sector. In addition to leading research at Coventry University, Alexeis has been course director for programmes including an MSc Cyber Security Management and an MBA Cyber Security.

Dr Mick Thurlbeck holds the position of Managing Director of Stapleton International. He is Visiting Fellow in Enterprise at the University of Sunderland within the Faculty of Business and Law having a key role Research in Innovation, Sustainability and Enterprise. Responsible for providing input to research projects and research development, teaching programmes and curriculum development, Mick also promotes the University of Sunderland internationally, particularly Singapore, Malaysia, China and Korea. Also holding an MSc in Quality Management, his experience includes being a Chartered Fellow of the Chartered Institute of Management and a Fellow of the Royal Institution of Naval Architects

Eddie How is a Security Risk Specialist. Based in Singapore, he actively engages the regional business leaders in geopolitical affairs, security and crisis management in the Asia Pacific region. Eddie has held various senior corporate function leadership position with Royal Dutch Shell PLC, NetApp Inc, Sun Microsystems and the Commercial & Industrial Security Corporation (CISCO), a former Statutory Board of the Ministry of Home Affairs before it was privatised in 2006.

1. Introduction

As in most other areas of the transport sector, the maritime industry has entered a new era of its evolution driven by developments in information technologies. During the last two decades a number of developments in the area of industrial control systems have dramatically changed the way ships, harbours, rigs and navigation systems operate and communicate. From the familiar mechanical systems that the industry once relied on, all infrastructure has now become a mixture of electromechanical constructs and highly integrated hardware and software forming a set of computer networks that cover the whole industry and communicate with many of its stakeholders (Tucci, 2017). The inclusion of software systems in ship design architectures has paved the way for the inclusion of new technologies and abilities that previously seemed impractical or too futuristic, improving navigation and everyday operation of vessels and structures within the maritime industry. In their interaction with other parts of the industry, modern ships have become communication hubs, entertainment centres, mobile-offices, learning spaces and much more (Mendes and Guerreiro, 2017). Connected ships are manufactured with hundreds of electronic control units (ECUs) and other in-built capabilities that allow direct access to the internet and enable them to consume, create, supplement, direct and share digital information with other ships and with maritime infrastructure such as harbours, ports and oil platforms and semi submersibles. Modern ships are highly sophisticated in their complexity with dozens of microprocessors running over 100 million patterns of control software. Major computing firms have already started creating processes that enable the integration of their systems with ships (Joszczuk–Januszewska, J., 2013). Connected ships can today be framed as a collection of complex software systems, subsystems and sophisticated components manufactured and developed by a multitude of geographically dispersed suppliers (Lam and Bai, 2016). This integration of a ship - one of the largest forms of hardware, with today's software is helping manufacturers compete and grow. This presents a very real a dilemma for the maritime industry; the positivity of the improvements in technology comes alongside the requirement to safeguard systems from external attack.

1.1 Cyber security and the maritime sector

With the new opportunities provided by the software systems and computer networks that support the maritime industry, a number of challenges have also emerged. The data and information driving the operation of the maritime infrastructure is exposed to malicious individuals and groups who pose a major risk for the security of the industry. In addition to having an awareness of the vulnerability of its digital resources, understanding where these digital risks arise and who can be responsible for them partly defines the cyber security of the industry.

Cyber security is a broadly used term, with highly variable, context-bound, often subjective, and at times uninformative definitions (Bay 2015, Cavelty 2012). There is a body of literature covering the term *cyber security*, what it means and how it is situated within various contexts. However, there is an absence of a concise, broadly acceptable definition that captures the multidimensionality of the concept (Tucker 2015, Craigen et al. 2014:4-10, Bishop 2005). Most attempts to define the concept have had the security of systems or individuals at its centre. Within the context of maritime infrastructure, cyber security will be understood as the protection of electronic systems, communication networks, control algorithms, software, users, and underlying data within the maritime infrastructure from malicious attacks, damage, unauthorised access, or manipulation.

1.2 The problem: the need for a holistic approach to cyber security in the maritime industry

The extant literature shows that research and practice on maritime cyber security has so far been aimed towards identifying different attack vectors capable of compromising mainly ships, harbour infrastructure and navigation systems. However, limited attention has been paid to the roles of the decision makers within the industry in gaining an understanding of the cyber vulnerabilities of the industry and its external threats (Bueger, 2015).

This paper argues that an holistic approach is required for the understanding and management of the cyber security of the maritime industry and outlines some of the different roles that decision makers play in that process. To address this, the rest of the paper is structured as follows: section 2 reviews the literature on cyber security and the maritime industry; section 3 introduces the concept of cyber security knowledge and highlights the need for a knowledge-based approach to cyber security

management in the maritime sector; section 4 provides our conclusions and recommendations for the implementation of the knowledge-based approach in the maritime sector.

2. The Maritime industry: cyber security landscape

The ship or vessel has a collection of several Independent Control Systems that coexist with a large number of legacy systems, all integrated into numerous onboard networks. Additionally the existing infrastructure network means ships are increasingly interconnected and also connected to other parts of the maritime infrastructure such as harbours and platforms and semi submersibles.

Maritime operations increasingly rely on such systems with direct and indirect access. Research has identified widespread exploitable vulnerabilities. The industry is rapidly adopting technology that is inherently insecure and improperly configured.

Criminals of various categories have demonstrated the motivation and capability to use blended cyber and physical attacks in ports and at sea. Limited reporting indicates terrorist cyber targeting of maritime operations, having already established their credentials in undertaking lethal seabourne operations.

2.1 Cyber Security Vulnerabilities:

The cyber threat to shipping is evolving; researchers have identified serious vulnerabilities, connected technology is emerging and criminals are realising the potential value of cargo. So far, attacks have included cyber elements with physical attributes, in so called "blended attacks." These attacks have occurred in locations and circumstances where cargo can be stolen, rather than held for ransom at sea. It is likely that known technical vulnerabilities may be targeted in future attacks.

Alongside the targeted threat, malware in its various guises is ubiquitous. In the last 18 months the use of ransomware, where files are encrypted and held hostage for payment, has become commonplace among criminal networks. There is a very strong potential that this could move into shipping.

2.2 Examples of Technical Vulnerabilities

- There are prevalent technical vulnerabilities in IT systems used shipping. Global Navigation Satellite Signals (GNSS) of the global position system (GPS) are known to have weak security measures and be susceptible to manipulation. These technologies, which update vessel position, have been jammed in UK government tests, resulting in ships moving off course. During experiments, the Electronic Chart Display and Information Systems (ECDIS) could not receive accurate positional data whilst linked to the autopilot. A device capable of exploiting GNSS weaknesses costs as little as $50 from illegal markets.

- Unencrypted and unauthenticated weak, signals for determining location are widespread. In a 2013 test by the University of Texas at Austin, a GPS spoofing device exploited the lack of authentication by legitimate inbound signals and overpowered them, leading to an $80m vessel's navigation system effectively being taken over.

- Experts assess these techniques may already be in use. Iran boasts that GPS spoofing capabilities and the interception of two US patrol boats by the Iranian navy off the Iranian coast in January 2016 was potentially facilitated by spoofing GPS signals to the craft.

- Electronic Chart Display and Information System (ECDIS) potentially susceptible to cyber attack. In January 2013, the USS Guardian grounded off the Philippines. Inaccurate data in the Electronic Navigation Charts (ENCs) was displayed on an ECDIS display. The data placed the reef nearly eight miles from its actual location. Although not a result of cyber attack, the accident demonstrates the growing reliance on digital mapping in automated systems and the potential impact of compromised ENCs.

- Automatic Identification Systems (AIS), used for vessel positioning and tracking are not protected by sophisticated encryption or authentication. Spoofing AIS signals could be used by vessel operators to disguise position or used to create false navigation obstacles.

- In 2014, potential vulnerabilities in Very Small Aperture Terminals (VSAT) for internet connectivity were identified and over 10,000 were discovered with open ports. Compromising a VSAT could be a first stage before pivoting to another part of the local network connected to the VSAT.

- Inmarsat and other satellite services are channelled through gateways in countries such as the US, Australia, Russia and China where they can be legally intercepted. Whilst this is mitigated out at sea, advanced nation-states can intercept satellite communications.

- The US Navy operated over 100,000 devices utilising outdated software. When Windows XP support was stopped owing to obsolescence, rather than replace the software the US Navy paid $9m per year for support to continue. A maritime security research company found even where new software is used, 37% of Microsoft servers failed to patch vulnerabilities.

2.3 Cyber Security threats

With the continuous ever expanding connectivity, remote access opens new opportunities for cyber attacks. The absences of non standardised or reliable data sharing protocols remain a major concern.

The lack of a Cyber Security Strategy for the industry has to be addressed as a matter of urgency. Common policies, procedures and processes are required to be developed and installed to reduce the threat attack to individual vessels, offshore installations, common maritime systems and onshore facilities. In addition to individual attacks the industry is also susceptible to acts of terrorism through breaches of security as noted below.

2.4 Terrorism

Al Qaida and other terrorist groups have stated intent and capability to attack vessels, perhaps best illustrated in the attack on the USS Cole off Aden in 2000 by al-Qa'ida in the Arabian Peninsula (AQAP). More recently, AQ-linked strategist Suleiman al-'Ali published a chapter on 'Maritime Jihad' in his online book, 'The Fall of the Idol'. He describes targeting commercial shipping as being the best path for Mujahiddin to gain control over the global economy.

Terrorist groups have increased their use of the internet for operational and radicalisation purposes, using it for encrypting operational communications and sharing radicalising content. Although their use of cyber attacks for destructive or disruptive purposes remains nascent, targeting maritime-related assets has been noted. In July 2016, the Caliphate Cyber Army released databases belonging to shipping companies. Three companies were targeted and data released on containers shipped into and out of the Suez Canal Container Terminal.

2.5 The need for cyber awareness

The increase of technology aboard vessels makes them more vulnerable to cyber attack. However, the relative isolation of essential systems from the internet makes shipping more difficult to compromise than other technologies (such as the internet of things). Therefore criminals and terrorists are less likely in the short-term to undertake cyber-only attacks, preferring comparatively easier targets.

Ransomware is the exception. Piracy operations have demonstrated the potential high rewards. Ransomware is less likely to put a crew and vessel in peril in the manner of piracy operations presently, but exploiting vulnerabilities to extort is likely to be of interest to criminals.

As with most operational environments without developed understanding of cyber attack vectors, the most likely introduction of malware will be inadvertent. Infected media being brought aboard and used to update equipment is a threat seen elsewhere in the enterprise.

Blended attacks are likely to continue to appeal to criminals and terrorists and develop in sophistication and audacity. The confluence of technology and physical attack is already present in terrorist and criminal operations. Monitoring terrorist adoption of destructive cyber capability should be considered with maritime threats in mind, given the continued interest in targeting shipping.

3. A knowledge-based approach to cyber security management in the maritime industry

In its ever-more connected and complex environment, the maritime industry has experienced remarkable technological changes within the last two decades. From the risks associated to the tens of thousands of suppliers that the industry relies on to the proliferation of mobile devices allowing staff to access vital information, exposure from a cyber security perspective now covers not only the industry and its supply chain but also the whole of the workforce. Such connectivity and exposure brings into the industry a significant degree of complexity.

If complexity is understood not only as the number of elements interacting within the digital domain of the maritime industry but also the non-linearity of their interactions (Egan et al., 2016). This makes of the cyber security of the maritime industry a highly dynamic concept.

3.1 Maritime cyber security: an unpredictable phenomenon

The cyberspace offers three key significant advantages to cyber attackers: relatively risk-free opportunities in the scale, space and time of cybernetics. In a context such as that of the maritime industry, the dynamics of the cyber security problem can then be defined by three main dimensions:

3.1.1 Scale

The scale of the impact of a cyber attack for the industry are beyond any other risks the industry has previously dealt with. Dombrowski and Demchak (2014) argue that cyber criminals can readily use the web to scale attacking units from small to large, tightly organised or loosely linked. Further, attackers can use the web for communication, training, supply, and operations, even as they scale up and down and back again.

3.1.2 Space

The space where cyber criminals operate is no longer a domain but the underlying layer on which modern society is built. For the maritime industry, the cyber space a critical infrastructure (Tucci, 2017) which underpins all operations.
As an environment imagined, created, developed, sustained, and extended by human intentions and actions (Dombrowski and Demchak, 2014), the variability of the space dimension poses a significant number of challenges to the industry.

3.1.3 Time

In contrast to the immutable or the slow-changing nature of its former challenges, the cyber security risks for the maritime industry change significantly over time. It is not only that the number of incidents in the maritime cyberspace continuously increase and in the last few years these account for a substantial part of operational risk incidents. The fact is that attacks can take place over time, which makes it difficult to identify and profile the attacker as well as understand the attack's high-level architecture (Rich and Buchanan, 2015).

3.2 Knowledge and a cyber security strategy

In these conditions, a key challenge for the maritime industry today consists of being able to devise an adaptive pathway to address the dynamics of its cyber security context. Adaptability to the changing nature of its cyber risks would allow the industry protect its online infrastructure from both random or organised attacks. Ultimately, all parts of the industry are required to improve their resilience to cyber incidents and -where possible, reduce their cyber threats.

To achieve these aims it is important for the industry to understand that a cyber security management strategy would be based to a large extent on assumptions. The variability and sometimes unpredictability of cyber security risks mean that any assumption made during the planning or analysis stage is likely to either be limited in its scope or soon become obsolete. An ongoing process of update of knowledge related to the cyber security landscape of the maritime industry is required for it to increase its cyber resilience.

Such a process would cover not only learning about the industry's own digital assets and their vulnerabilities, but also understanding the external cyber threats (including those associated to its supply chain) an the impact that attacks targeting specific assets may have in the operation of the industry. That continuous process of learning, sharing and reusing cyber security knowledge within the maritime industry can be defined as maritime cyber security knowledge management.

Maritime cyber security knowledge management would allow the industry to provide an adaptive response to the diversity of issues that it encounters in the digital domain. It would include a number of complementary roles and responsibilities to be delivered by the industry's management board, which would:

- Support the industry in managing the overall risk of a successful cyber attack on its infrastructure and operations.
- Support the industry in encouraging all players (e.g. employees and also suppliers and maintainers, contractors etc.) to ensure that appropriate defences and resilience against cyber attacks are built into the systems and products they supply.
- Support development of further training and documentation on cyber security, including further guidance and industry-developed detailed operational guidance.

4. Conclusions and recommendations

As the development, introduction and refinement of digital infrastructure becomes even more prevalent within the maritime industry, there is increased optimism surrounding the many benefits such changes are bringing. Transformation in work practices, controls and management are being generated and enjoyed by all parties to such an extent that both management an on-board crew are benefitting greatly from technological advancement. The challenges associated with the introduction of such innovative management systems and the requirement to implement necessary controls and effective measures to ensure that cyber security may be effectively maintained is fundamental to the future success and safety of the industry.

Earlier detailed examples of the vulnerabilities and threats effectively highlight the fact that the marine cyber security landscape has an urgent need for an effective industry-wide cyber security management strategy. Agreement, development and implementation of such a strategy is not without obstacles. In addressing the need for change and the objective of achieving a compliant model for all parties, across the diverse industry leading to the introduction of the variables is a major task in itself. Coupled with the dynamics of cyber security highlights the need for an effective industry-wide cyber security management strategy.

The introduction of a suitable strategy for cyber security knowledge and its management could provide the industry with the adaptive pathway to better understand the dynamics of the cyber security problem. This in turn will facilitate an improved level of protection of online infrastructure from random or organised attacks.

Future work will develop a model that outlines the principles of a cyber security knowledge management strategy for the maritime industry. The developed model will assist the industry in understanding the requirements for the future.

References

Tucci, A.E., 2017. Cyber Risks in the Marine Transportation System. In *Cyber-Physical Security* (pp. 113-131). Springer International Publishing.

Bueger, C., 2015. What is maritime security?. *Marine Policy*, 53, pp.159-164.

Dombrowski, P. and Demchak, C.C., 2014. Cyber war, cybered conflict, and the maritime domain. *Naval War College Review*, *67*(2), p.70.

Egan, D., Drumhiller, N., Rose, A. and Tambe, M., 2016. *Maritime Cyber Security University Research: Phase 1* (No. CG-D-07-16). US Coast Guard New, London United States.

Joszczuk–Januszewska, J., 2013,. Importance of Cloud-Based Maritime Fleet Management Software. In International Conference on Transport Systems Telematics (pp. 450-458). Springer Berlin Heidelberg.

Lam, J.S.L. and Bai, X., 2016. A quality function deployment approach to improve maritime supply chain resilience. Transportation Research Part E: Logistics and Transportation Review, 92, pp.16-27.

Mendes, J. and Guerreiro, M. 2017. Conceptualizing the cruise ship tourist experience. *Cruise Ship Tourism*: 205.

Thomas Rid a.nd Ben Buchanan, 2015. Attributing Cyber Attacks, *Journal of Strategic Studies*, 38:1-2, 4-37