Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector

Kimberly Tam, Kevin D Jones

Maritime Cyber Threats research group, University of Plymouth, UK

ABSTRACT

Standard risk assessments are used to define and prioritize threats within a sector. However, the rising number of cybersecurity risks in maritime are often temperamental to a range of environmental, technical, and social factors. A change during an incident can significantly alter the risks and, consequently, the incident outcomes. Therefore, agile, changing risk profiles are becoming more necessary in the modern world. In addition to static and dynamic, maritime operational risks can be affected by cyber, cyber-physical, or physical elements. This demonstrates the equal use of information and operational technology (IT/OT); however, most quantitative risk assessment frameworks focus on one or the other. This is not ideal, based on technological trends in the maritime sector. This article explores the factors that affect maritime cyber-risk and examines popular risk frameworks to see whether important maritime-related elements are unaccounted for. These findings are further examined with the results of a survey we conducted to assess the situational awareness of the sector around cyber-risks in maritime. Suggestions for future work on are then made based on our findings.

Keywords: Situational awareness, risk, maritime, information technology, operational technology, cyber-physical, IoT, autonomy

1 INTRODUCTION

The maritime transportation sector, worth trillions, moves 90% of the world's goods using widespread port infrastructure and fleets of unique, often specialized, ships. These ships traverse international waters and carry tons of cargo and millions of passengers every year. Better technology on-board and at port continue to improve operations, however, it exposes assets and people to a complex, diverse, range of cyber-risks. Overall, the top maritime risk is considered to be "business interruptions" (Allianz, 2018). However, more recently as technology improves, cyber risks in the maritime sector are rising quickly to pose a considerable threat, jumping from 15th to 2nd highest risk in just five years (Allianz, 2018). While a significant shift in risk, the situational awareness of the sector is still lacking. In a recent survey conducted by the authors (see Appendix Q17), participants believed by 78% that raising the general situational awareness of maritime cybersecurity would help reduce risk. This is important, as the vulnerabilities of modern ships and ports could lead to massive losses. While the recent Costco (Rajamanickam, 2018) and Maersk (Maersk, 2017) incidences have drawn attention to the importance of cyber-risk management in the maritime industry, there is still little understanding on what that means, fully, or how that should be establish.

In the past, when other industries have faced similar increases in cyber-risks, many adopted methods of risk assessment and mitigation based on an awareness their unique issues. In this aspect, the maritime sector is behind the curve, partially due to a slower embrace of technological advancement. This gap is quickly closing, however, with even more maritime technology changes in the near future (see Section 5). This sector has now reached the point where must, more seriously, gain better situational awareness and risk assessment capabilities. To gather more information on both topics, this article explores how maritime cyber risks are different from other sectors, and evaluates general awareness of the risks by conducting, and sharing results of, our maritime cyber-risk survey. Generally speaking, quantitative risk assessment is popular for managing risk and has been used to analyse only the physical risks to maritime ships (Chai, Jinxian, & Xiong, 2017). The first step to better risk assessment, is to address the gap in understand between physical risks and cyber risks, specifically in maritime. Second, most assessment methods have the disadvantage of being entirely static, failing to adapt as risks change. This lack of dynamic assessments has contributed loss of life (BP, 2005), and is another area we wish to increase awareness in.

While existing risk-assessment methods evaluate physical risks, maritime must also include the newer cyber-aspects of risk. This assertion is made based on the survey conducted as a part of this paper to understand what influences maritime risks. In summary, the purpose of this article is to:

1) Improve the situational awareness of the maritime risk landscape;
2) Examine how maritime risk can be modelled in terms of cyber, physical, static, and dynamic factors;
3) Determine if the necessary elements are accounted for in existing risk assessment frameworks;
4) Discuss survey results and future work.

For our third aim, this article examines three risk assessment frameworks; the National Institute of Standards and Technology, i.e. NIST, (Gary, Alice, & Feringa, 2002) (Stouffer, Pillitteri, Lightman, Marshall, & Adam, 2015), Failure Mode and Effects Analysis (Lui, Lui, & Liu, 2013), and MaCRA the Marine Cyber-Risk Assessment (Tam & Jones, 2019b).

2 BACKGROUND

Cybersecurity in the modern maritime industry is still a relatively new concept (BIMCO, 2016) with individuals becoming more aware as Information Technology (IT) and Operational Technology (OT) systems evolve across ships and at port. Land based port infrastructure itself has had its largest advancements centered on IT. On ships and offshore structures, however, IT and OT have been upgraded more equally over the last few years, often converging. While the sector as a whole is very familiar with using physical risk assessments, there has been little awareness raising, or action, against cyber-related risks. The purpose of this section is to understanding the current state of technology in maritime, current risk assessment methodology, and the sector's current awareness levels of the problem. These concepts will then be broken down further in the following sections.

2.1 RISK ASSESSMENT METHODOLOGY

Risk assessment methods can typically be divided into two core methods, qualitative or quantitative. Qualitative assessment prioritizes individual risks through the analysis of occurrence probabilities, while quantitative numerically analyses risk by assigning numerical risk values. The majority of current maritime risk assessments, for physical-based risks like collision, are based on probability statistics. These have been, and still are, very reliable as they supported by an extensive history with many statistics (Jakub, et al., 2014) (Nordstrom, et al., 2016) (Goerlandt & Montewka, 2015). Conversely, it is the lack of history and situational awareness of cyber-related risks in

maritime that makes it very difficult to produce qualitative risk assessments for maritime cyber-risks. Currently there very little data because of limited reporting abilities (Tam & Jones, 2019a) as well as a short history.

Since there is not enough historical maritime cyber incident data for qualitative assessments, and there will not be enough data in the future either if awareness and practices are not improved soon, this paper focuses on quantitative approaches. The pros and cons of quantitative depend on the quality of elements being modelled or assessed; their relevance, the quantity, set size, and overall coverage. When done right, quantitative approaches can be more objective when derived from solid facts. When done poorly (e.g., the financial market in the early 2000's) a limited set of modelled elements means the model is unable to consider unusual, tail end, risks. Quantitative models often reduce these issues by choosing a smaller, and very specific scenario to analyse (Flammini, Gaglione, Nicola, & Pragliola, 2008) (Chai, Jinxian, & Xiong, 2017). These also often limit the risk analysis problem to a specific asset, geographic location (e.g., harbour), or outcome (e.g., oil spill).

A quantitative risk model that encompass more elements can be more detailed and versatile; however, the performance overhead could reduce its usefulness. In addition, if complex models rely heavily on humans there is the potential that human errors can be introduced. Complex models can also be difficult to understand, but it has been shown that graphical outputs like CORAS (M. S. Lund, 2010), can mitigate that issue for users (K. Labunets, 2014).

2.2 MARITIME TECHNOLOGY

The maritime sector as long been a critical component in modern global transportation and trade. In its past, piracy and other physical threats were a common threat, and so assessing those threats is well established. Risk factors like geographic location (e.g., Strait of Malacca), cargo value, and defences (e.g., armed guards) helped individuals assess the risks of certain voyages. The introduction of electronic and digital systems began with sonar on ships at the start of 1900's, which was quickly followed by more digital systems across the sector. On the shore side of business, shipping was actually one of the first business to embrace computers to keep track of ledgers and the tables of the UK Nautical Almanac. Each new system introduced decrease workloads, increased accuracy, and improved physical safety. The negative aspect to the then speedy growth was the development of a complex computing environment with no cybersecurity built-in. This created vulnerabilities in both IT and OT both technically and through human-system interactions. Unlike the cyber aspect, human error in maritime has been studied in some depth (Wingrove, 2016) (Rothblum, 2000).

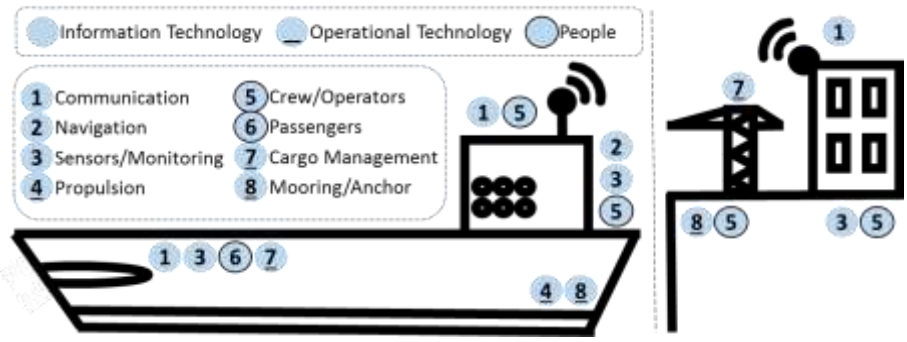

Figure 1 IT, OT, and human elements on-ship and at port

As ships grew larger and more sophisticated, as seen with the evolution of the modern oil tanker since the 1870's, the growth of containerization since the 1970's, and the evolution of passenger ships, the maritime risk landscape has changed due to all the new cyber and cyber-physical risks. This article defines cyber-physical threats as events with both cyber and physical elements (Tam & Jones, 2018b) which come from the emergence and convergence of information technology (e.g., anti-collision software) and operational technology (e.g., autonomous cargo winches). All the physical operations required in maritime transportation means the amount of physical and cyber factors are fairly even, particularly when compared to more IT-orientated businesses like finance. The convergence of IT/OT most closely mirrors other transportation sectors like rail and air; however the magnitude of cargo volume and distance/time travelled is significantly higher in the maritime sector. Lastly, the most recent introduction of internet, complex networking like Internet-of-things and wireless communications has compounded the existing cyber-related risks in maritime (see more in Section 5). Figure 1 illustrates how IT/OT/human elements are relatively, evenly, distributed across ports and ship. Here the categories of the IT and OT systems are relatively generic and may encompass several systems while providing background information, with details are to come later.

3 Relevant Maritime Risk Factors

This article has briefly discussed IT (e.g., data sharing), OT (e.g., physical operations), and the human element in a maritime environment. These three have been considered the top categories of risk factors; however, each element belonging to these categories can be further categorized into static or

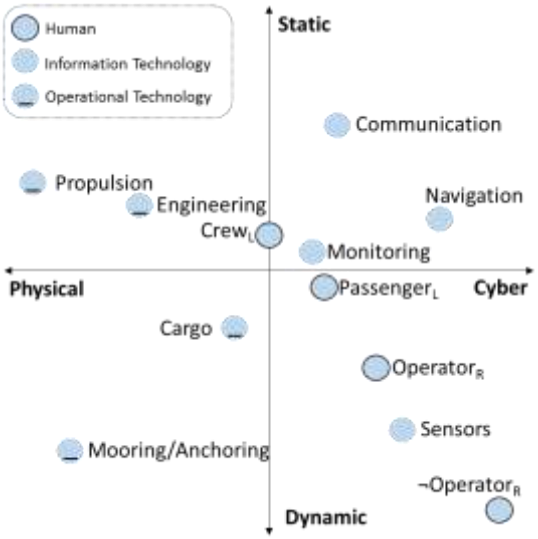

Figure 2 Risk factor compass demonstrating range of elements involved

dynamic, and physical or cyber factors that should be modelled to assess risk. This is particularly important in the maritime environment today, with the rise of cyber-physical systems (Stankovic, Lee, & Sha, 2010). This detail of element categorizing is unusual in related works, and will allow this research to assess how effective existing risk assessments can be for maritime. It also raises situational awareness on how complex and unique the maritime cyber threat is, even compared to other transportation sectors like rail, car, and air.

The risk factor compass in Figure 2 summarizes the following subsections by organizing elements of risk ranging across the physical, cyber, static, dynamic spectrum. It also demonstrates how human, IT, and OT are biased to certain quadrants of the compass due to their inherent natures. For example, OT systems tend to provide physical actions, and remote humans tend to affect dynamic cyber risks more than local crew or passengers. This demonstrates how the unique set of these risk factors can create a distinct maritime risk landscape, one that is larger than what is currently addressed. This is because the current situational awareness of cyber-risk is often fragmented into only human, IT, or OT categories and not assessed together. Part of raising awareness on which risks require more attention is understanding potential attack outcomes. The types of risk outcomes considered in this paper, which can be applied to human, IT, and OT entities, are denial-of-service (DoS), misdirect, damage, theft, and obfuscate. Ultimately, these risks can result in outcomes such as loss of finance, loss of life, and environmental damage.

3.1 Static

Each of the following subsections for static, dynamic, physical, and cyber factors will discuss how they affect risks within the human (H), IT and OT risk categories established earlier on. For the interested reader, more details on human threats can be found in (BIMCO, 2016) (Tam & Jones, 2019b).

For the purpose of this paper there are four types of human categories, local on-ship crew ($crew_L$), remote operators working on land ($operators_R$), on-ship passengers ($passengers_L$), and the remaining, remote, non-operator people ($\neg operators_R$). Local crew and passengers on the ship mean their physical safety is tied to the ship's location and safety. As these people are unlikely to leave a ship mid-voyage, their history prior boarding are static factors. For crew this includes their training, which is based on set standards. While training standards change with the times (Wingrove, 2016), and there are slight variations across different cohorts and countries, the training for a crew member is relatively static at the point they are on a ship, as they are unlikely to receive significantly new training on-route. Conversely, while individual histories are static per voyage, people often disembark and embark at ports, meaning static is relative to the period examined. Static human factors are important as they establish previous criminal records or vulnerabilities (e.g., health, finance). Assessing human risk with both static and dynamic risk factors has been done previously in (Bonta, 1999) and (Beech, Friendship, Erikson, & Karl, 2002), although not applied directly to maritime, where static factors include history and dynamic factors include substance abuse. A significant shift in maritime that shall occur in the future is remote control and autonomy (Yeomans, 2014), which may alter crew risk factors towards remote operators instead of local crew. Of the remote non-operator people, we must consider hackers and how they affect maritime cyber-risk.

Much like how the amount and types of people on-board differ between ship types (e.g., cruise, cargo), on-board IT systems can also vary. However, because of standards set by the IMO International Convention for Safety of Life at Sea (IMO, 1974), ships of similar types are mandated to have standard IT systems. This is primarily determine by tonnage (e.g, gross tonnage), local or international waters, and the presence of passengers. Systems found in this sector can be loosely categorized into computers, navigation, cargo handling, communication (e.g., human to human, machine to machine), sensors, and monitoring. The last two were previously combined in Figure 2 as they possessed similar capture and network technology, however, their risk factors diverge more when considered in depth. Because of existing standards, the static factors of IT systems are primarily their hardware, established networks, and protocols to use those networks. Changes to these

factors happen less often than crew and, even if hardware is upgraded, the ship is unlikely to undergo these alterations during normal operations. Instead, retrofitting normally stalls normal operations. Therefore, the main risks to consider with static elements, is "inherit" vulnerabilities in the supply-chain and during maintenance. Such risks could be structural, where systems are physically vulnerable, or a cyber-vulnerability where a back door was intentionally or unintentionally built in for intruder access.

When considering OT, this paper makes a distinction between hardware and mechanisms, although the latter could be considered a subset of the former. Here, the term hardware is used in the computing sense while mechanisms, like a propeller or winch, perform physical services. We must also differentiate between propulsion and engineering, unlike Figure 2. While the figure considered them nearly identical in terms of function and physical location on-board, risk factors in engineering have a much more diverse outcome and has more crew interaction. This differentiation may be even more pronounced in the future, as ship engineering OT is becoming more sophisticated and converging with bridge IT (Man, Lundh, & MacKinnon, 2018). Risks from these static features tend to result in accidents, as the vulnerability is constant, while dynamic factors can be changed to trigger an attack. A flaw in computer hardware or OT mechanisms could lead to a damaging event, while a shortcoming in crew training could result in the mishandling of technology. For example, there was a rise in engineering-related accidents after a global shift to a new type of fuel (Allianz, 2018).

3.2 Dynamic

Being able to re-assess risk factors as they change is critical when analysing risk over a period of time. In maritime, as voyages can take weeks or longer, and the life cycle of ship is an average of 20 years (ICS, 2018), at least 5 years more than the average aircraft. Over such spans of times, elements are likely to change and the speed at which technology evolves today is quick. Therefore, to fully analyse relevant shipping risks across a number of ships, environments, and scenarios, dynamic factors must be considered. Based on our survey, compared to static, there is less awareness of dynamic risks.

When assessing the dynamic risks contributed by the human element, for those involved with shipping operations, remote and local, it is important to consider changes in "health", i.e. mental, physical, and financial. Threats to these could make an individual vulnerable to blackmail, manipulation by a malicious party, or become a malicious entity. Examples of sextortion and blackmail have been seen on ships, as well as disgruntled employees becoming insider threats and passengers accidentally leaking information

(ESCGS, 2015) (USACIDC, 2017). These factors can change at any time, triggered by an event such as a fishing email. This is a common event on-shore (e.g. at a port), but also happens on a ship. Over a 5-day period, maritime mail gateways scan a million messages, 31,836 of which are spam and 2,196 contain actual malware or viruses (GTMaritime, 2017). Besides non-crew and non-passenger, the risks of interest are malicious third party hackers (Tam & Jones, 2019b). Therefore, the dynamic elements worth measuring are their resources and goals, which can easily change.

The primary dynamic factors for risk when considering maritime IT systems is their software and use. The majority of IT ship systems, particularly those situated on the bridge (e.g., ECDIS, AIS, GMDSS, SSAS), are single purpose. The primary example is ECDIS (Electronic Chart Display and Information System), which runs on a normal PC with an underlying OS (CyberKeel, 2014). This OS, normally Windows but occasionally Linux, has the capacity to do many things but is used purely for executing ECDIS as a navigation aid. Limited access to the underlying OS reduces risks, however, there are enough use-cases (e.g., updating charts) and misuse cases that can affect risks dynamically. Unlike navigation, communication, monitoring (e.g., CCTV), and sensors have a plethora of applications. Moreover, the design of sensor networks and the cost/simplicity of individual sensors today means that sensor networks are versatile, dynamic, and growing fast. This is becoming more relevant with Internet-of-Things (IoT) in maritime, particularity in smart container tags for shipping. How sensor readings are made and stored, and how they affect decisions (i.e., man-made and machine-made), affect the risk of the ship. This includes cargo, which can be temperature sensitive or motion sensitive, people (e.g., carbon-dioxide levels), and the ship's physical and cyber safety. Dynamic risks are currently better monitored in onshore businesses, as companies often employ active intrusion detection systems etc.

The dynamic factors of operational technology are similar to IT in that they are also dependent on how they are accessed and controlled by other systems and people. Unlike IT, however, the amount of OT being operated by humans is much lower, as it often is limited to a subset of the local crew, as they require training and access permissions. Very few OT systems allow remote control at this point in time, whereas ship IT systems are more connected to the Internet. This may change especially if more ships trend towards autonomy. As OT systems interact with the physical world, dynamic risks also include ship surroundings, such as sand banks and port structures. As the ship moves and environments change, these factors for measuring risks are uniquely dynamic in transportation sectors, such as maritime. As there is less awareness on ship-side risks, we tend to focus more on these aspects.

3.3 Cyber

Measuring cyber risk is more established across other sectors, particularly financial, government, and IT companies. In comparison, even to other transportation sectors, very little has been done in the maritime sector which has been estimated to be 20 years behind cybersecurity trends based on the rate of technological integration and current state of forensic and mitigation capabilities (Tam & Jones, 2019b). Moreover, the unique systems, protocols, and the movement across physical and cyber spaces mean that traditional methods of risk assessment cannot be easily applied without heavy modification. However, the basic concept of communications human-to-human, machine-to-human, and machine-to-machine still affect risk. For human-cyber interactions, the factors to measure for risk are human identifications and security (e.g., IDs, passwords), who they communicate with, and how. For remote operators and hackers this is the primary risk element to analyse. This is also a significant factor for local crew and passengers with easier, local, access. This same connection can be used to exploit people and propagate viruses (GTMaritime, 2017) (USACIDC, 2017).

Regarding IT, specialized navigation systems like ECDIS have a set of protocols for using local networks and the Internet. This limits the risks to the use of those protocols, and the security of the network. Specialized communication technology like marine radio also have fixed use protocols, which can limit the possible risks. The simplicity of many of these systems still add a layer of "security", as they are sometimes too simple for a pure cyber-attack. However, this does not discount the possibility of using vulnerabilities to enable social engineering, blurring IT and human risks. For more versatile networks, those hosting sensors, cameras and internet-based communications, they must consider user ID, passwords and user permissions. Particularly for CCTV and other sensitive monitors or sensors, access control is an important part of managing risks. The human element is also key here, as the rate and extremes of crew change are unique to a ship's crew. Not only is the timing and number of crew changes significant, but on international voyages the nationalities of the people can vary significantly. Hence, these elements would have a dynamic element as well.

Of the three categories, OT on ships and at ports are the least Internet connected. This does not mean that they are not connected to some kind of network (e.g., SCADA) or that this may not change in the future (Man, Lundh, & MacKinnon, 2018). Access to these kinds of networks are mostly done at specific terminals, currently primarily locally or in engineering instead of an IT system central, like a ship bridge. Even these networks have known vulnerabilities, but because of the current access requirements, it is

really only local crew that can affect these risks. SCADA and similar networks types enable digital communications, although not with the same bandwidth and reach as the Internet, which can contribute to maritime cyber-risks. This can be seen in similar, yet different, studies of SCADA security in other sectors like water, power, and rail (Cherdantseva, et al., 2016). Because operational technology have both physical and cyber elements, their presence, scale in size, and uses mean that maritime security is equally, and uniquely, cyber and physically orientated when considering risk.

3.4 Physical

The last category of factors that affect maritime risk to be discussed in this paper are those in the physical category. Here the risk for operators, local and remote, and passengers is measured by their physical health and the devices they bring on board. This is becoming more important today with bring your own devices (BYOD) to work and the increase use of smart phones and USB enabled devices (e.g., cameras, flash drives) that can spread malware. For physical outcomes, other risks can be tied to lithium batteries and other device components that can cause a physical hazard. For all human risk elements, location is another risk factor. For some this is static, as most cyber-attackers and remote operators do not change their physical location. However for people on a ship, their location is dynamic which may alter the risks involved. For example, close proximity to terrorist or high-congestion zones will affect different risks. Lastly, the human element affects IT/OT physical security as local crew, and sometimes passengers, can physically affect systems.

For both information and operational technology, there are physical components that affect risk and are affected by risks. The computing hardware of the systems need physical access security as well as cyber-access security. In addition, systems that may be exposed to harsh environmental factors, like engine-focused sensors, have different risks. This can also include sensing devices designed to monitoring volatile or hazardous cargo, or to measure the wind and water externally. The main difference between information and operational technology when considering physical risks is that, again, OT relies less on computing hardware and more on mechanisms like motors, robotic arms, and winches to perform tasks like propulsion and cargo handling. Furthermore, there is currently less automation with OT devices, requiring more physical interactions and command sequences from crew. However, this may change as technology improves, as discussed in Section 5. Because OT interacts heavily with the environment (e.g., mooring to a pier, unloading cargo to a truck), physical elements that affect risk must be considered in order to fully assess maritime risks. In addition to Figure 2, Table 1 lists examples of factors in all these categories.

Table 1 Categories and examples of maritime cyber-risks on ships

	Risk Factor	Static	Dynamic	Cyber	Physical
Human Element	$Crew_L$	training, history*	health, resources	ID/password, internet use	location, health, BYOD
	$Operators_R$	training, history*	health, resources	communication	health
	$Passenger_L$	history*	health, resources	internet use, communication	location, health, BYOD
	¬$Operators_R$	history	resources, incentives	internet use, communication	location
Information Technology	Navigation	protocols, hardware	software, use	software, network use	hardware (e.g., AIS)
	Communication	protocols, hardware	software, use	ID, software, access	hardware (e.g., SSAS)
	Sensors	hardware, network	devices*, use, software	network, access	hardware, locations
	Monitoring	hardware, network	software, use	access control, network	hardware, access
Operational Technology	Propulsion	hardware, mechanisms	use, environment	terminals, communication	mechanisms (propeller), access
	Cargo	contents*, history*	environment (temp)	tags, internal sensors	location, health
	Moor/Anchor	mechanisms, crew*	protocols, environment	protocols, communication	mechanisms, location, crew
	Engineering	crew*, mechanisms	environment (temp)	protocols, communication	mechanisms (engines), environment, crew

* - static if single voyage, dynamic if assessing longer period of time

4 Assessments and Key Survey Results

The aim of Section 3 was to expand the current awareness on what factors affect maritime cyber-risks. With that, it is now possible to evaluate how well existing tools can assess these all of these relevant factors; cyber, physical, static and dynamic. A useful assessment framework should also be able to prioritize risks, to determine the top risks so they can be dealt with immediately. Establishing the abilities of existing tools will help further increase situational awareness and risk mitigation in this sector. A useful tool should also be user-friendly, to aid human decisions. Understanding whether the discussed risk frameworks meet these goals will guide recommendations on how maritime risk mitigation can be improved, including suggestions for adapting to likely future changes in the technology aboard ships and ports, such as increased autonomy, remote control, or the use of augmented reality.

4.1 Risk Assessment Framework Comparison

The frameworks examined here are NIST, FMEA, and MaCRA. There are many NIST frameworks for assessing various risks, however, this article will focus on NIST's management of IT systems (Gary, Alice, & Feringa, 2002) and industrial control systems (Stouffer, Pillitteri, Lightman, Marshall, & Adam, 2015). The latter is very similar OT systems; however this tool is specialized to a smaller manufacturing and distributions worksite, not entirely suitable for port-like infrastructure. After a brief analysis and comparison, the next subsection on situational awareness uses the results of a cyber-risk survey, with participants primarily from the maritime sector, to support claims. The full survey results can also be seen in the Appendix. Many existing frameworks also suggest using a number of specialists to combat risk. The problem with this is the scope of possible risk, even on-board, can be daunting. It would be unreasonable to expect those levels of expertise on-board, which is another issue to consider. Lastly, the targeted audience in the NIST documents are predominately high-level management and security experts, which is less relevant to the range of audience types actively interested in maritime security (see Q1 in Appendix) and FMEA results can vary hugely depending on the investigation team.

In terms of covering all relevant risk factors, the NIST IT risk framework nominally ignores OT and assumes that all physical and network security, once established, is set or static. However, as we have seen, that assumption would not hold if systems are on moving ships. Another concern is that the two NIST frameworks are would require extensive work to be combined in order cover both physical and cyber risks. Moreover, the ICS risk framework is not versatile enough to assess OT maritime risks, and the IT framework is only suitable for business IT, which means a combined framework would likely not cover the full range of cyber/physical risks found in maritime. Another noticeable drawback of NIST frameworks is the lack dynamic risk measurements. This has been a factor in OT incidences, or more specifically ICS, with some more severe outcomes including loss of life (BP, 2005).

Similarly, FMEA does not consider dynamic features, however, this is more clearly by design, as its purpose is to identify all possible failures in a design, process, product, or service in its early stages of design or re-design (Lui, Lui, & Liu, 2013). This makes FMEA a useful assessment tool for inherent flaws, or what this paper has labelled as static risk. This makes FMEA and NIST useful in static risk assessment, physical or cyber, but less so with dynamic risks. However, both these frameworks use gradients of risk in order to rank the risks they do analyse and prioritize risk management strategies. While highly effective in most environments, because of the wide range of risks in

Table 2 Comparing Risk Assessment Frameworks for Maritime

	NIST	FMEA	MACRA
Cyber Risks	✓✓	✓	✓✓✓
Physical Risks	✓✓	✓✓✓	✓✓
Static Risks	✓✓✓	✓✓✓	✓
Dynamic Risks	✓		✓✓✓
Well established	✓✓✓	✓✓✓	✓
Appropriate audience	✓	✓	✓✓✓

✓= some, ✓✓= yes, ✓✓✓= yes and integrated into framework

maritime cyber, they may be less effective. If done thoroughly, FMEA could mitigate the dynamic risks once a ship is released, however, mitigating every risk no matter how minor is not cost effective, and during the lifetime of a ship significant unseen risks can arise as global circumstances change.

Unfortunately, the human element plays a minor role in the NIST and FMEA frameworks. Again, NIST has a separate framework (i.e., SP 800-53 Personnel Security) and it is not clear whether, if combined, they could cover the range of risks discussed for maritime. FMEA has branched into human error (e.g., health-care), but it is also considered a separate use and not integrated with IT/OT assessments. While future ships may shrink crew sizes, it is highly unlikely that crew will be completely removed from the sector. It has been estimated that autonomous ships, with all life support systems removed, can reduce operational costs significantly (Morris, 2017), however, if a passenger ship already requires human safe conditions it is not worth the considerable risk of running those ships without a crew.

The last framework evaluated is MaCRA, which in comparison is more theoretical but also more maritime orientated (see Table 2). This framework is relatively new and not well established, however it was destined specifically for maritime as awareness grew for this subject. Much focus has been placed on measuring dynamic risks as technology evolve (Tam & Jones, 2018a) and as ships travel. A drawback of this framework's early stages of development is the lack of widespread data to populate the model fully. While an effort has been made to assess features in the maritime context, MaCRA does not assess static risks as thoroughly as FMEA, as those are established outside of shipping operations. A combined method may be possible, as FMEA would not need to be applied to maritime context, but instead be used to assess the manufacturing plants, processes and supply.

4.2 SITUATIONAL AWARENESS

This survey conducted for this research (see Appendix) explores the idea that maritime cyber-risk is a mix of cyber, physical, static and dynamic elements and participants confirmed that these were relevant when assessing the risks of ships and ports. Therefore, it is important to modify existing frameworks to work in the maritime ethos, or to continue develop maritime-specific frameworks until they are equally well known and usable. Participants were relatively evenly split into "I have a good awareness", "I have moderate awareness" and "I have limited awareness" of cybercrime threats in the maritime industry. However, in total, "little to no awareness" was ranked highest around 36%, and 78% of all participants claimed that raising general awareness of the topic would effectively reduce the risk of cyber-attacks.

This survey consisted of 22 questions regarding maritime security factors, training, and use. Of the 75 participants, 65% of them were mariners and port officers, roughly 14% were trainers/trainees, and the rest were primarily higher management and high ranking security specialists. Participant minorities included maritime servicers, equipment providers, regulators, insurers, IT system owners or support, and academics. It is important to note that less than 15% of these participants identified themselves as being a part of the targeted audience of the two NIST frameworks this article has examined. Moreover, FMEA primarily targets manufactures only, meaning it is applicable to roughly 5% of those who were interested enough in maritime cybersecurity to take this survey. While 41% of participants were not familiar with risk assessment in general 22%, however, knew of NIST. The majority of participants said no (44%) and with 11% listing alternatives.

Of these participants, 74% ranked crew-training standards as the top problem, with cybercrime and attacks ranking at second with 55% (Appendix Q2). Moreover, 60% of participants said that they have not received any training in cybersecurity, and participants ranked the need for maritime cyber training at 75 out of 100. Concerning cyber incidences, participants thought IT was the most vulnerable technology at 50%, however 41% believed IT and OT were equally, and significantly, at risk. This demonstrates how situational awareness around physical-cyber risks need to be raised, and how both IT and OT need to be considered when assessing risk. As described previously, NIST assesses IT very well, but is less capable of assessing IT/OT and humans blended together and, therefore, less applicable to maritime.

According to participants, their top three cybercrime concerns are malware (31%), phishing scams (13%) and web-based attacks (13%) (see Appendix Q11). Other surveys have had similar results (IHS, 2018) (Daszuta & Ghosh,

2018) (Daszuta & Ghosh, 2018). However, these surveys rarely asked about what factors play into these risks. Even though these concerns seem primarily IT-based, and therefore can be solved with IT cybersecurity solutions, in the maritime sector a wide range of physical, dynamic factors must be considered. While ship computers and internet activity are ranked as critical cyber-factors by 79% of participants, over 50% of participants also identified geo-location, route, cargo, crew, and insider threats as factors in risk (see Appendix Q10). These identified elements can be categorized as dynamic or static factors. More results can be found in the Appendix, to raise more awareness on how complex assessing maritime cyber-risks, across ships, ports, international lines, etc., can be. In section 5, the future of technology of maritime will be discussed followed by some recommendations for improving cyber-risk awareness, analysis, and mitigation in the maritime sector.

5 FUTURE RESEARCH DIRECTIONS

Before discussing future actions in maritime cyber-risk and sector-wide situational awareness of the risks, it is important consider the future of maritime technology in first, as it significantly affects future risks.

5.1 FUTURE MARITIME TECHNOLOGY

This section explores a few technologies and concepts that are gaining popularity in the maritime sector. This aims to provide a cyber-risk perspective, particularly in the growing number of dynamic cyber aspects.

Digital Twins

More shipping companies are investing into the new "digital twin" concept. Sophisticated simulations of a physical asset (i.e. ship) drive this cost saving concept by creating a suite of simulations models that can interact on a common platform. This platform would allow a number of simulation models to be loaded at one time and to interact with each other, allowing for a highly customizable platform for a multitude of analyses. The primary aim of this is to improve operational efficiency and costs. However, in terms of cybersecurity, the digital twin cannot easily enhance cybersecurity or risk analysis capabilities. This is because only a few ship attributes are simulated and the simulation would not have the same cyber vulnerabilities as an actual ship. Conversely, the digital twin itself could introduce issues. While less likely and difficult to achieve, as digital twins consist solely of virtual parts and exists only in cyber-space, its digital files could be targeted in a cyber-attack to affect decisions and actions. In summary, while the digital twin will improve the building and monitoring of ships, it is unlikely to have significant positive, or negative, effects on how to assess maritime cyber-risks.

Table 3 Modified SAE autonomous car terms for ships

	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
Ship Autonomy	No/minimal autonomy. Small crew required.	Partial automation e.g. auto pilot.	Conditional autonomy, potential interventions by crew	Ship is mostly self-running. remote crew rarely required.	Complete autonomous operations in all potential settings.
Remote operations	Not required	Not required	Not required, but likely	Required for operations	Not required
Sensors / IoT	Needed to aid crew decision	Needed to aid crew decision	Needed to aid crew and autonomy decision	Needed to aid remote crew and autonomy	Needed for complete autonomous decisions

Autonomous Ships and Ports

Because of the growing demands on the maritime sector, many in the shipping industry have begun to consider autonomy as a solution. Autonomy can be achieved at different levels of sophistication, and while there are established levels for autonomous cars, there is no formal definitions for the levels of autonomy in ships. An adaption of SAE autonomous car definitions to ships can be found in (Tam & Jones 2018a) and in Table 3. Because of the challenges in automating the various systems on board a ship, to perform a wide range of operations, it will be a while before fully autonomous ships represent a significant percentage of the global fleet (Batalden, Leikanger , & Wide, 2017). However, despite the technological and legal complexities, the potential reductions of operation costs annually (estimated up to 90%) makes autonomous ships a desirable capability for future trade. Besides technical challenges like autonomous navigation, international laws and the risk of the lost cargo and lives have complicated the progress toward fully autonomous ships, much like the struggle for autonomous cars. Because of this, many organisations are currently working with lesser degrees of autonomy.

Remote access and control, as discussed in the next subsection, will most likely be used in mid-tier autonomous ships. With roughly 2GB of data stored per day on a modern ship (Brandy, 2018), autonomous vessels at tier 3 and tier 4 will likely generate even more data to support machine learning control algorithms or constantly feed data to remote crews. While tier 3 autonomous ships may potentially have a reduced local crew that can analyse data and react, with a minimal crew it is likely that a remote specialised group will perform more complex operations that use remote access. This can result in communication-based vulnerabilities, when data can be altered or denied.

However, data could also be altered while stored on the ship or at a remote location. With tier 4 autonomy, it is likely that both remote access and control will be implemented since higher tiers aim to fully remove all local crew and rely minimally on remote help. Conversely, with tier 5 autonomy the ship operates fully autonomously, self-directing, and does not require assistance from remote crew. However, it is unlikely any ship owners would not have contingency options considering the value of the ship and cargo. It is likely that remote operations are possible, used less frequently at tier 5.

Currently there are more autonomous ports in full operation than there are autonomous ships. In these ports, cargo is handled primarily by advanced OT systems (Rebollo, Julian, Carrascosa, & Botti, 2019) (Wilshusen, 2015). Unlike autonomous ships however, a highly autonomous port will still have human supervision and maintenance, as the cost savings are less dramatic when compared to autonomous ships. In other words, the cost savings of removing the human element from ports is not worth the risk. In the future, however, ports are likely to increase the number of autonomous services they provide, especially as other ships become more autonomous. For example, if autonomous ships are easier to direct, port congestion is likely to increase and more autonomous traffic management may be needed to support human-based decisions. The majority of all the autonomous ports in existence also primarily deal with cargo ships and containers. This was a relatively easy first step, as containers have set dimensions, weight, and already have machine-readable data such as origin, contents, etc. As ports and ships develop, there is a drive for other autonomous services, such as autonomous operations for oil and gas. This industry is striving towards fully autonomous operations by 2030 to 2035 (Venables, 2018), especially as hundreds of oil and gas structures, in the marine environment, approach decommissioning (Jones, Gates, Huvenne, Philips, & Bett, 2019). Additionally, smaller ports and offshore structures may also incorporate more autonomy as time passes.

The number of devices that the maritime sector could contribute to the worldwide network is extensive, as discussed in the IoT subsection. In particular, the rise of autonomous ships and ports will mean more sensors and devices are needed to support all operations (Brandy, 2018). With increased more automation, monitoring and actions such as invoicing and moving cargo will generate, and require, more digitally collected data, drastically increasing the number of IoT devices. If sensors and other monitoring devices become the only source of information for human and computer-based decisions, the cybersecurity of the individual sensors themselves come into question. In such cases data integrity becomes imperative, and so more secure storage and data transfer must be provided as autonomous technology develops.

Remote Operations, Connections, Virtual Reality

As discussed previously, there are various, growing, levels of autonomy in ships and infrastructure like ports. Autonomy, however, can be seen as a set of several developing technologies, many of which could be considered significant trends themselves in the maritime sector. For example, remote communications, remote-enabled control, virtual reality, and augmented reality. While there are several machine-to-machine and human-to-human communication connections in maritime operations (e.g., satellite, marine radio, internet), the types of cyberattacks and vulnerabilities are similar due to the nature of wireless transmissions. Regardless of how remote access or control signals are sent, those transmissions are vulnerable to jamming attacks (Tam & Jones, 2019b). Additionally, if the protocols are insecure, spoofing and leaks can occur if data is altered or stolen. Besides the technical vulnerabilities in digital connections used in maritime, the human element at sea and shore can be vulnerable. Particularly if crew become more remote and staff primarily oversee operations, attacks that hide or misrepresent data can negatively alter human behaviour. The use of virtual reality as a remote control aid could present this kind of IT/human risk. Hence, it is important to make sure digital connections are trustworthy and to set up contingencies if a communication channel is lost or determined to be untrustworthy.

Augmented reality, unlike remote operations and full virtual reality, has potential uses for displaying digital information at ports but, more likely, at sea. Disregarding security, augmented reality could display more information in a human-friendly manner (Baldauf & Procee, 2014). If displaying this data locally, this moderately mitigates the vulnerabilities mentioned above. However, augmented reality shares the same misinformation risks that can cause people to make harmful decisions since virtual objects are less easily verifiable. If a cyber-attack is able to alter relevant data, the likelihood that the false data is discovered before causing an incident goes down. This type of risk has been speculated about before with eAtons, virtual markers that could be spoofed to cause an accident (Tam & Jones, 2019b). Considering the emergence of newer technology, augmented systems for ships could widen the range of accident outcomes, as there could be more ways to trick people. For example, using augmented navigation systems in areas difficult to navigate (e.g., shifting ice without physical markers), can make navigation much easier. More specifically, artic waters have highlighted the benefits of virtual beacons and augmented reality for ships (Frydenberg, Nordby, & Eikenes, 2018). In this case, a misinforming change to the data fed into augmented reality programs could shift the correct shipping lane on the screen enough to increase the probability of a collision if the crew is not vigilant.

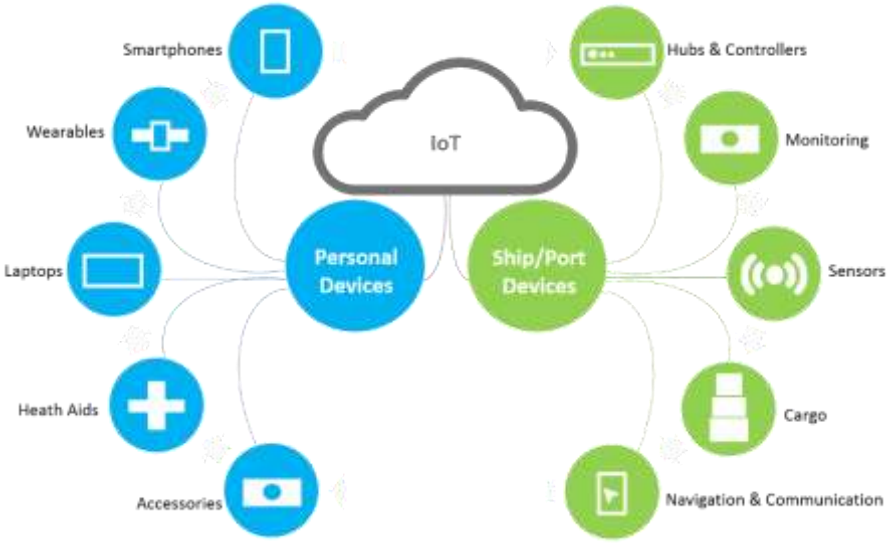

Figure 3 Likely categories of devices within a maritime Internet-of-Things

Internet-of-Things

The Internet-of-Things (IoT) concept is that many types of devices are interconnected, via the Internet, and sharing significant amounts of data. As this definition is extremely broad, IoT networks in the modern world are inherently massive and complex when considering the number and types of internet-connected devices available. Specific to maritime, in a recent survey, trends showed that 42% of maritime organizations believed they would benefit from additional IoT solutions and 2.5 million dollars will be spent on IoT over the next three years, more than either cloud computing or big data analytics (Brandy, 2018). Again, cost savings are driving IoT solutions in maritime, with predicted cost savings up to 14% over the next five years. Specific to this sector, IoT devices can be categorized broadly into personal, ship, and port devices. As illustrated in Figure 3, personal and ship/port devices are separated because personal devices are generic technology in a maritime context, while ship and port devices are more bespoke to the maritime sector. The underlying technology may be more commonplace; however, this does result in different cyber risks. For example, while ships and planes may use similar navigation systems, they diverge enough that the security risks will differ, in addition to the different contexts they are used in.

Both IoT personal devices and devices on ships are considered physically mobile. Therefore, in addition to adding a cyber-element of risk, they also add a dynamic geographical risk as devices connect to a number of local and international network nodes. Because maritime IoT devices will be mobile across several networks, including different internet laws, hardware, users, and owners, this drastically increases the risk possibilities. The often constant communications between these devices across the Internet introduce several vulnerabilities to the overall IoT. It is important that these risks be addressed as more devices are connected and as operations become more dependent on the connectivity. A network is also as secure as its most vulnerable device, therefore access and permissions must be set accordingly. Sensor-based devices (e.g., wind, temperature, vibration) in maritime are also used differently and exposed to different hazards. While many sensors are, and will be, installed in control areas like the bridge, many are also placed in engineering. For volatile or sensitive cargo (e.g., natural gas, medication, food) it is likely more IoT devices will be introduced for cargo maintenance. An increase of monitoring devices would help support a number of machine and human based decisions across a ships and ports, as seen in in Figure 1. This diversity is what separates ship and port devices most from more traditional IoT devices, and defines the unique aspects of a maritime IoT.

Some of the significant benefits of IoT comes from data analytics and the access to a wealth of information from multiple sources. As mentioned previously, cargo management supported by IoT-enabled tags may revolutionize the shipping industry (Weber, 2010). Not only would this have significant effects on the entire industry, if implemented globally, considering the volume of cargo shipped around annually, maritime devices could become the biggest device contributor to the worldwide IoT. It has been reported that a single modern shipping ship can host 5,000 data tags and 3,000 sensors in the main control and engine rooms (Brandy, 2018). These IoT devices found in these areas can be seen on the "ship-device" section of Figure 3's IoT diagram. The number and diversity of devices today, as well current level of maritime cybersecurity skills, have contributed to 87% of mariners believing their IoT security could be improved. This would mean that a significant percentage of the future global IoT would be dedicated to maritime operations, which could have significant effects on the cybersecurity across other sectors. Another factor that could lead to maritime devices dominating the IoT space would be if more ships and ports decided to use more remote control, remote access, or autonomy, as those would require more sensors and monitoring devices, and more communication devices, to compensate for a less humans, or no humans at all (Tam & Jones, 2018a).

Environmentally Friendly Fuel

In addition to safer sustainable operations, another area of focus for emerging technology in maritime is protecting the environment. Newer IMO regulations have changed maritime operations for this purpose, such as max speeds; however, more solutions are being implemented or suggested every day. Technical solutions that change what kinds of energy is collection (e.g., tide, solar, eco-fuel), storage, and use, will have effects on cyber-risks. By potentially harvesting from multiple energy sources, such as offshore wind or on a ship, energy storage and distribution systems must be able to cope with several inputs, as well as more outputs, and be able to control the flows of energy with high precision. Especially on a ship, which is often isolated and stricter with energy consumption, a smart grid may be necessary to manage fuel and energy. With power systems using converging IT/OT, there will be more interconnectivity with multiple sensors and external systems. This would continue to widen the range of cyber risks. Energy must be produced and stored safely to prevent hazardous outcomes, and the transfer of energy must be correct to ensure optimal operations and safety. For example, correct monitoring and distribution of energy would prevent certain systems from overloading or systems malfunctioning because they are not receiving enough power. As these renewable energies, smart grids, and eco-fuels continue to change ship operations, it is important to note the potential cyber risks.

5.2 UNDERSTANDING AND MITIGATING RISKS

While risk assessment, even cyber-risk assessment, share similarities across different industries, differences in technology (IT and OT), environments, and human users do significantly change the risks. To fully understand and mitigate risks in each sector, a certain amount of situational awareness is required. As seen in our survey, those in the maritime sector believe that maritime cyber awareness levels need be increased, as well as cybersecurity training at all levels of employment (e.g., seafarer, management). In addition to the survey results, this paper looked at the physical, cyber, static, and dynamic factors that do affect risks in this sector. In addition, this paper then looked at three risk assessment frameworks for maritime to see if they analysed all of these factors. From these observations, we make three suggestions for future research paths into understanding and mitigating risks.

We suggest improving the situational awareness of maritime cybersecurity by, firstly, changing human awareness using training, research, and talks to spread awareness. This may influence policy and standards of practice. In addition, incorporating new technologies like augmented or full virtual reality into normal day operations or training should be made secure. That said, many previous attempts at increasing awareness sector has been hindered by the

lack of information. Therefore, another related area of research should be devoted to acquiring data relating to maritime cyber-risks and threats. One way of doing this is improving forensic readiness (Tam & Jones, 2019a) in order to gather and analyse ship and port information that is relevant to cybersecurity. This has a more specific outcome to general big data analytics, which have so far been focused primarily on shipping operation efficiency and pricing. Lastly, we encourage risk assessors to be aware of the limits and strengths of the methods they are applying to cyber-risks in the maritime sector. Even within this sector, there is a significant diversity in ships, ports, operations, and national/international standards. Understanding if combining or adapting risk models is necessary would further improve safety.

6 CONCLUSION

The maritime sector represents a significant, global-wide, part of modern life. Although the sector as a whole has tended to be technologically behind even other transportation sectors, it is quickly embracing maritime-specific technologies like autonomous shipping, and making potentially massive impact on future technology. This sector is not unaccustomed to assessing risks, as physical risks have existed since the beginning. However, moving forward, physical and cyber risks need to be assessed together as well as dynamically over time. This article demonstrated the importance of adopting this by highlighting the types of factors (i.e., human, IT, OT, cyber, physical, static, dynamic) that affect cyber maritime risk. This article further evaluates the current situational awareness and three existing risk assessment frameworks (i.e., NIST, FMEA, MaCRA) using the four types of risk elements discussed and results from a survey we conducted. This helped us further conclude that there is no well-established risk assessment method that is completely adequate for maritime, and made observations and suggestions that may improve awareness and solutions toward maritime security.

7 REFERENCES

Allianz. (2018). *Allianz Risk Barometer.* Allianz Global Corporate and Specialty SE.

Allianz. (2018). *Safety and shipping review.* Alianz Global Corporate and Speciality SE.

Baldauf, M., & Procee, S. (2014). Augmented REality in Ships Bridge Operation.

Batalden, B., Leikanger , P., & Wide, P. (2017). Towards autonomous maritime operations. IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA).

Beech, A., Friendship, C., Erikson, M., & Karl, H. (2002). The Relationship Between Static and Dynamic Risk Factors and Reconviction in a Sample of U.K. Child Abusers. Sexual Abuse: A Journal of Research and Treatment.

BIMCO. (2016). The Guidelines on Cyber Security onboard Ships Version 2.0. *International Chamber of Shipping, INTERTANKO, BIMCO and CLIA and ICS and INTERCARGO and*.

Bonta, J. (1999). Approaches to offender risk assessment: static vs dynamic. *Research summary Vol. 4 No. 2*.

BP. (2005). *Fatal Accident Investigation Report.* Texas City: Isomerization Unit Explosion Interim Report.

Brandy, D. (2018). IoT in Maritime - Inmarsat Research Programme. SVP Market Strategy, Digital Ship, CIOLondon Forum.

Chai, T., Jinxian, W., & Xiong, D.-q. (2017). Development of a quantitative risk assessment model for ship collisions in fairways. Saftey Science.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). *A review of cyber security risk assessment methods for scada systems.* Computers & Security, vol. 56.

CyberKeel. (2014). *Security Risks and Weaknesses in ECDIS Systems.* NCC Group Publication Maritime Cyberwatch.

Daszuta, W., & Ghosh, S. (2018). Seafarers' perceptions of competency in risk assessment and management: an empirical study. WMU Journal of Maritime Affairs.

ESCGS. (2015). Maritime Cyber Security White Paper: Safeguarding data through increased awareness. *ESC Global Security Cyber Security White Papers*.

Flammini, F., Gaglione, A., Nicola, M., & Pragliola, C. (2008). Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures. International Conference on Critical Information Infrastructure Security.

Frydenberg, S., Nordby, K., & Eikenes, J. O. (2018). Exploring designs of augmented reality systems for ship bridges in artic wters.

Gary, S., Alice, G., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. NIST 800-30.

Goerlandt, F., & Montewka, J. (2015). Maritime transportation risk analysis: Review and analysis in light of some foundational issues. Reliability Engineering & System Safety.

GTMaritime. (2017). *Cyber Security in the Maritime Industry*. Retrieved from https://www.gtmaritime.com/cybersecurity-maritime-industry/

H. H. Safa, D. M. (2016). *Cyber security of smart grid and scada systems, threats and risks.* CIRED Workshop.

ICS. (2018). Review of Maritime Transport. *International Chamber of Shipping, United Nations Conference on Trade and Development (UNCTAD)*.

IHS. (2018). BIMCO, Fairplay, and ABS Maritime Cyber Survey 2018 - the results.

IMO. (1974). International Convention for the Safety of Life at Sea. International Maritime Organization.

Jakub, M., Ehlers, S., Goerlandt, F., Hinz, T., Tabri, K., & Pentti, J. (2014). A framework for risk assessment for maritime transportation systems—A case study for open sea collisions involving RoPax vessels. *Reliability Engineering \& System Safety*.

Jones, D., Gates, A., Huvenne, V., Philips, A., & Bett, B. (2019). Autonomous marine environmental monitoring: Application in decommissioned oil fields. *Science of the Total Enviroment.* Elsevier.

K. Labunets, F. P. (2014). *An experiment on comparing textual vs. visual industrial methods for security risk assessment.* Empirical Requirements Engineering.

Lui, H.-C., Lui, L., & Liu, N. (2013). Risk evaluation approaches in failure mode and effects analysis: A literature review. Expert Systems with Applications.

M. S. Lund, B. S. (2010). *Model-Driven Risk Analysis: The CORAS Approach.* Springer Publishing Company Inc.

Maersk. (2017, August). *A. P. Moller Maersk improves underlying profit and grows revenue in first half of the year*. Retrieved from https://edit.maersk.com/en/the-maersk-group/press-room/press-release-archive/2017/8/a-p-moller-maersk-interim-report-q2-2017

Man, Y., Lundh, M., & MacKinnon, S. (2018). *Managing unruly technologies in the engine control room: from problem patching to an architectural thinking and standardization.* WMU Journal of Maritime Affairs.

Morris, D. (2017). *World's First Autonomous Ship to Launch in 2018*. Retrieved from \url{http://fortune.com/2017/07/22/first-autonomous-ship-yara-birkeland/

Nordstrom, J., Goerlandt, F., Sarsama, J., Leppanen, P., Nissila, M., Ruponen, P., & Lubecke, T. (2016). Vessel TRIAGE: A method for assessing and communicating the safety status of vessels in maritime distress situations. *Safety Science*.

Rajamanickam, V. (2018). *COSCO's cyber attack and the importance of maritime cybersecurity*. (FreightWaves) Retrieved from https://www.freightwaves.com/news/technology/coscos-cyber-attack-and-the-importance-of-maritime-cybersecurity

Rebollo, M., Julian, V., Carrascosa, C., & Botti, V. (2019). *A multi-agent system for the automation of a port container terminal.*

Rothblum, A. (2000). Human Error and Marine Safety. *International Workshop on Human Factors in Offshore Operations.*

Stankovic, R., Lee, I., & Sha, L. (2010). Cyber-physical systems: The next computing revolutionv. *Design Automation Conference*.

Stouffer, K., Pillitteri, V., Lightman, S., Marshall, b., & Adam, H. (2015). Guide to Industrial Control Systems (ICS) Security. NIST 800-82r2.

Tam, K., & Jones, K. (2018). Cyber-Risk Assessment for Autonomous Ships. *C-MRiC Cyber Security .* IEEE.

Tam, K., & Jones, K. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. Journal of Cyber Policy.

Tam, K., & Jones, K. (2019). Forensic Readiness within the Maritime Sector. IEEE C-MRIC Cyber SA, Oxford.

Tam, K., & Jones, K. (2019). MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment. *Technical Report*. WMU Maritime Affairs.

USACIDC. (2017). Cyber Sextortion. *U.S. Army Criminal Investigation Command, CPF 0002-17-CID361-9H*.

Venables, M. (2018, Dec). *Five Steps To Autonomous Operations For Oil And Gas*. Retrieved from Forbes: https://www.forbes.com/sites/markvenables/2018/12/31/five-steps-to-autonomous-operations-for-oil-and-gas/#319700b47c64

Weber, R. (2010). Internet of Things - New security and privacy challengers. (p. Vol 26). Computer Law & Security Review, .

Wilshusen, G. (2015). *Maritime critical infrastructure protection: DHS needs to enhance efforts to address port cybersecurity.* GAO-16-116T.

Wingrove, M. (2016). Lack of training causes ship accidents and detentions. *Marine Electronics and Communications*.

Yeomans, G. (2014). *Autonomous vehicles handing over control: Opportunities and risks for insurance.* Lloyd's.

KEY TERMS

Cyber-Physical: the relationship and combination of cyber and physical in risks, vulnerabilities, and incident outcomes.

Hardware/Mechanisms: computer hardware and OT mechanisms.

Maritime Cyber: the intersection of cyberspace and maritime technology

Risk Factors: elements or factors that can positively or negatively affect certain risks and can be modelled to show that

Situational Awareness: sector-wide perception of issues relating to cyber-risks within their environment.

BIOGRAPHICAL NOTES

Professor Kevin Jones: earned a B.Sc. (Hons) in Computer Science from the University of Reading, a M.Sc. in Computation from the University of Oxford, and a Ph.D. from the University of Manchester. Kevin is a Fellow of the Institute of Marine Engineering, Science and Technology, the Institution of Engineering and Technology and the BCS – The Chartered Institute for IT. He is a senior member of the Institute of Electrical and Electronics Engineers. He is the Executive Dean of Science and Engineering at the University of Plymouth, with research interests in the domain of Trustworthiness of Complex Systems, particularly maritime cybersecurity.

Dr. Kimberly Tam: gained a B.S in Computer and System Engineering at Rensselaer Polytechnic Institute in the USA and a PhD in Information Security, focusing on smartphone malware, from Royal Holloway University of London in the UK. She is currently a Research Fellow on maritime cybersecurity, focusing on risk assessment.

REFERENCE

Reference to this paper should be made as follows: Tam, K., & Jones, K. 2019. (2017). Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector. *International Journal on Cyber Situational Awareness*, Vol. 2, No. 1, ppxx-yy

Appendix – Survey Results

Q1: Please can you tell us which of the following most closely matches your role?

ANSWER CHOICES	RESPONSE
Seafarer	32.00%
Ship Security Officer	2.67%
Ship owner	1.33%
Ship Manufacturer	1.33%
Trainer	6.67%
Trainee/Student	14.67%
Maritime Service/Equipment Provider	2.67%
Regulator/Insurance	2.67%
Senior Management	10.67%
Chief Information Officer	2.67%
Designated Approving Authority	1.33%
IT Security Program Manager	0.00%
Information System Security Officer	1.33%
IT system owner or support	2.67%
Other (please specify) Responses	17.33%

Ages:

< 21	(1.9%)
21-30	(34.6%)
31-40	(9.62%)
41-50	(11.5%)
51-60	(25%)
> 60	(17.3%)

Q2: What in your opinion, are the biggest problems facing the Maritime Industry? Please select up to five.

74.6%	Standards: crew training
55.2%	Cyber crime/attacks
44.0%	Environmental restrictions
35.8%	Piracy
25.5%	Over capacity of certain ships (e.g. containers)
20.9%	Terrorism
14.9%	Falling price of oil
13.4%	Charter Price

Q3: Which ship systems do you think are most vulnerable?

50%	IT
41.9%	Both IT/OT equally
8%	OT

Q5: Are you familiar with risk assessment frameworks (e.g. NIST)?

44.3%	No
23%	Yes - NIST
21.3%	Maybe
11.5%	Yes – Not NIST

Q6: Have you received any training in Cyber Security?

60.7%	No
39.3%	Yes

Q7: Do you believe that generic Cyber Security training would be useful for your tasks?
72/100

Q8: Do you believe that maritime specific Cybersecurity training would be useful for your tasks?
75/100

Q9: Please choose the one that you agree with most:

32.8%	I have limited awareness of maritime cyber threats
32.8%	I have moderate awareness of maritime cyber threats
31.2%	I have a good awareness of maritime cyber threats
3.4%	I have no awareness of maritime cyber threats

Q10: Please select all elements you think have an effect on maritime cyber (cyber-physical) risks.

70.7%	Ship computers
58.6%	State-level outsider threat
50.7%	Firewalls
46.6%	Location/Route
44.8%	Cargo (value, type…)
39.7%	Intrusion detection
67%	Crew
22%	CCTV
50%	Insider threat
50%	Prankster: outsider threat
41%	Company espionage
74%	Internet activity

Q11: In your opinion, which Cyber Crime threat is most likely to occur in the Maritime Industry?

31%	Malware
17%	Unsure
13.9%	Web based attacks
13.9%	Phishing/spear-phishing
8.6%	Denial of service attacks
6.9%	Malicious code
5.3%	Malicious insiders
3.5%	Stolen Devices

Q12: In your opinion, which Cyber Crime threat causes (or could cause) the most financial damage to the Maritime Industry?

24.1%	Malware
13.8%	Unsure
13.8%	Denial of service attacks
13.8%	Malicious code
12%	Web based attacks
10.3%	Phishing/spear-phishing
6.9%	Malicious insiders
5%	Stolen Devices

Q13: How do you think a Cyber-attack would become apparent on a ship? Please choose up to three.

37.9%	No obvious symptoms
37.9%	Communication failure
34.5%	GPS failure
25.9%	Loss of navigation
24%	External notification
15.5%	Poor track keeping, intermittent faults
12%	Black out
8.6%	loss of engine control
8.6%	Other

Q14: Do you know who to inform after a Cyberattack?

60%	Yes
40%	No

Q15: What actions do you think can be taken to reduce Cyber Risks?

63.6%	Firewalls
58.2%	Provide duplicate and independent back-up systems
52.7%	No external devices allowed into sensitive areas (bridge)

43.6%	Restrict use of personal devices
40%	Monitor external communications
7.3%	Other

Q16: What actions do you think you would take after a Cyber Attack?

67.3%	Engage independent backup-system (if fitted)
30.9%	Get vessel to safe position and anchor if possible
24.6%	Switch systems off and re-boot to start again
23.6%	Continue to nearest port or point of refuge
18.2%	Other (inform external technician or company)

Q17: What actions can the industry take to reduce risk of Cyber-attack?

78.2%	Raise general awareness
58.2%	Carry out cyber security audits on board
41.8%	Vessels to carry Cyber "Health" certificate
54.6%	Duplicate / independent back-up systems
10%	Other (training, IDS, shore-based help)

Q18: How would you test ship security after an attack?

85.7%	Shore-based experts to visit vessel and prove security
33.9%	Internal investigation
16.1%	Generic advise to wipe/re-start systems
3.6%	Other

Q19: Have you or someone you know been the victim of a maritime cyber incident?

78%	No
22%	Yes

Q20: If known, please choose the closest cause of the incident.

61.5%	Malware (Malicious Software – Ransomware, Viruses, Worms, Trojan Horses)
15.4%	Denial Of Service Attacks (An interruption of an authorised user's access to a computer network)
15.4%	Phishing and Spear Phishing Scams (The mimicking of a genuine company to entice Individuals to reveal personal information)
7.7%	Unknown
0%	Malicious Insiders
0%	Web – Based Attacks
0%	Stolen Devices

Q21: If known, please select the known outcomes from the incident.

15.4%	Delays
15.4%	Information loss
15.4%	Physical loss
15.4%	Finance loss
15.4%	Unknown
7.7%	Information corruption
7.7%	None
7.7%	All of the above
0%	Reputation damage