The Maritime Industry and the Cyber-'Iceberg'

Rossouw von Solms[1,3] and Suné von Solms[2,3]
[1] School of IT, Nelson Mandela University, South Africa
[2]Department of Electrical and Electronic Engineering Science, University of Johannesburg, South Africa
[3]South African International Maritime Institute, South Africa

rossouw@mandela.ac.za
svonsolms@uj,.ac.za

Abstract: The maritime industry is embracing cyber technology. The proliferation of digitalisation in the shipping industry is apparent, as any modern vessel today is a complex cyber-physical-mechanically engineered system. The digital incorporation of operational technology (OT) and information and communication technology (ICT) systems in network and control systems has resulted in complex integrated shipping vessels. As most modern vessels utilise the internet to communicate with those on shore, it is true to say that shipping today has adopted cyber technology to enhance the efficiency of its operations. It is also true that the modern shipping industry has become totally dependent on cyber technologies for its future existence. Along with the integration of ICT and cyber-related technologies came numerous cybersecurity threats. These risks need to be identified and mitigated. If not properly addressed, these underlying cybersecurity threats can lead onto disasters of all different kinds. This paper discusses the integration of (ICT) and cyber-related technologies in the maritime and shipping industry, the related cybersecurity threats encountered and why these should be mitigated. It also suggests how senior management and the crew members can contribute in assisting to safeguard shipping vessels from these ever-present cybersecurity threats.

Keywords: Maritime Industry, Cybersecurity, Iot, Cyber Threats, Governance, Cybersecurity Education

1. Introduction

No longer is a shipping vessel at sea far away from numerous dangerous threats. No longer are the operational technology systems, that control the multiple mechanical systems on-board a shipping vessel, removed from any off-board danger. No longer is a shipping vessel a micro, artificial floating 'ecosystem' whilst it is at sea.

The advancement of the shipping industry has led to the continued integration of computing equipment, information technology, sensors, etc. with the operational technology systems on-board modern shipping vessels. This has changed shipping forever.

Various operational technology systems communicate continuously with many critical information technology systems, on- and off-board, resulting in a critical myriad of digital data that control the well-being of the vessel, the freight and those on-board. This critical digital data has become the lifeblood of most modern vessels, flowing through highly interconnected digital networks (veins).

Cyberspace has changed the way in which the modern world operates, doing business, communicates, relax, etc. Perhaps slower than other industries, but the maritime industry is catching up and utilising the benefits cyberspace has to offer. Along with the numerous benefits cyberspace has to offer came the myriad of cybersecurity threats that need to be avoided and mitigated.

The objective of this paper is to assess, evaluate and assist the efforts to successfully integrate cybersecurity, specifically from a human point of view, into the modern maritime industry. This will be done by studying the advancement in the shipping industry over years. The integration of ICT in modern shipping will be highlighted, followed by typical vulnerabilities of using ICT and cyber technologies in the shipping industry. Cybersecurity in the modern maritime industry will be highlighted and compared to a typical iceberg of old. Lastly, two important human-related remedies will be presented.

2. Advances in the Maritime Industry

The utilisation of water faring vessels dates to ancient times, where seafaring vessels were used for a variety of purposes, including exploration, trade, warfare, fishing and mobility. The challenges provided by the maritime environment, such as propulsion, communication, navigation, safety and security have led to a range of technological advancements throughout the centuries. In general, however, it is believed that the shipping industry has been slower to integrate technological developments compared to on-shore companies, but in

recent years the industry has seen the steady adaption and inclusion of technology (Abi-Saab, 2018; Voyager, 2023).

Ship propulsion is one of the cornerstones of the maritime industry and remains an indispensable part of global trade, exploration and connectivity (Kundu, 2023). Before the 19th century, ship propulsion relied mainly on oars and wind, were the industrial revolution brought forth the use of coal-fired steam engines, enabling ships to move faster and more reliably, greatly advancing global trade. The diesel engine replaced steam, which is now slowly being supplemented with green alternatives such as Liquefied Natural Gas (LNG) engines, Diesel-electric and Hydrogen solutions (Kundu, 2023; Maritime Cyprus, 2020). This landscape not only underwent updates in power and propulsion technologies, but recently started to include and utilize more sensor technologies, data processing and autonomous control, which replaced many of the manual tasks, like monitoring and metering and decision making (Matuszak, 2021).

Historical navigation heavily relied on celestial navigation techniques, using stars and celestial bodies as guides, coupled with compasses for directional orientation at sea. These traditional methods laid the foundation for more sophisticated navigational tools. The introduction of radar technology marked a pivotal shift in maritime navigation during the 20th century. Radar enabled vessels to detect other objects, coastlines, and potential hazards, significantly enhancing situational awareness (Hegland et al, 2017). The integration of Global Navigation Satellite Systems (GNSS), such as Global Positioning Systems (GPS), revolutionized navigation by providing accurate positioning information globally (Kaplan & Hegarty, 2006). The advent of Electronic Chart Display and Information Systems (ECDIS) ushered in a new era of digital navigation, where ECDIS combines electronic navigational charts with real-time navigation information, offering dynamic and interactive displays for enhanced route planning and safety (Baldauf et al, 2016). The recent integration of Artificial Intelligence (AI) and Machine Learning (ML) into navigation systems now aims to refine decision-making processes, optimizing route planning and collision avoidance (Moussavi et al, 2020).

The communication field is widely considered the area where technological advancements have been embraced. Starting at the traditional methods such as maritime signal flags, technological innovations have revolutionized maritime communication, where radio communication is seen as a pivotal milestone. Radio technology significantly enhanced real-time communication between ships and shore, contributing to safer navigation and efficient coordination (Smith, 2018). The emergence of satellite communication systems transformed maritime connectivity which enabled seamless communication across vast ocean expanses, ensuring continuous contact and data exchange for vessels at sea (Rao, 2019). The integration of satellite technology has not only improved the reliability of communication but has also facilitated the implementation of advanced navigation systems, enhancing overall maritime safety and efficiency.

Historically, maritime safety relied on traditional practices and rudimentary equipment, but contemporary developments have ushered in a new era of comprehensive protection. The integration of Automatic Identification System (AIS) technology has been instrumental in enhancing maritime safety. AIS enables vessels to broadcast their identity, location, and course, facilitating real-time tracking and collision avoidance (Hui et al, 2019). Additionally, the adoption of Unmanned Aerial Vehicles (UAVs) and satellite surveillance has expanded the scope of maritime monitoring, enabling authorities to respond proactively to potential threats (Arreola-Risa et al, 2017). Furthermore, developments in biometric technologies have strengthened access control measures, ensuring that only authorized personnel have entry to critical maritime spaces (Saeed et al, 2021).

In recent years, the maritime industry has witnessed a surge in the adoption of digital technologies. The Internet of Things (IoT) and sensor networks have enabled the collection and transmission of real-time data, allowing for more informed decision-making on vessels (Wang et al, 2020). Additionally, the advent of autonomous vessels and smart shipping technologies is ushering in a new era of maritime communication, where vessels can communicate, navigate, and operate autonomously, further optimizing efficiency and safety (Yang et al, 2021).

3. Integration of ICT and Data Usage in Modern Shipping

With the proliferation of ICT, numerous IoT systems and sensor equipment throughout the operational systems of modern vessels, data is continuously being captured, analysed, stored and transmitted. Only now this data becomes useful to the ship and related industry (Lind-Olsen, 2019). Obviously, the capturing, analysing, storing and transmission of this data need to be done in a very reliable manner.

The transmission of data to and from the shore has become critically important (Lind-Olsen, 2019). The smart and intelligent usage of ICT and IoT systems on and off the ship and the flow of data to and from enable effective

shore-based operations with the likes of maintenance service providers, customer support centres, port authorities, among others (Lind-Olsen, 2019). These vast amounts of data allow for clever analysis and integration into decision-making at various levels to the advantage of the ship, those onboard, the freight and the holding organisation (Moan, 2022).

The advantages that modern ICT and IoT offers enable ship owners and operators to meet the demands and expectations of customers and to deliver on global expectation (Moan, 2022). Digitalisation and the clever use of ICT does not only contribute operationally to the maritime industry, but also strategically. Value is added to make operations at sea smarter, safer and more sustainable (Larsen, 2020). Shipping companies who set out to harness the power of 'big data' and advanced analytics will gain strategic advantage on competitors (Larsen, 2020).

From the above it is clear that data plays an integral role. As mentioned, data gets continuously captured, analysed, stored and transmitted to be used in decision-making and for other important operations and purposes. Following are some examples of areas where data gets used lately:

- Improving vessel performance

  The continuous monitoring of and reporting on data captured from systems such as the vessel engine, electrical power, climate control, etcetera assists in optimising the performance. Therefore, data related to aspects such as; revolutions per minute, fuel and oil flow rates and temperature changes is important to capture, analyse and use (Julius, 2016).

- Supply chain management

  Electronic sensors are used extensively used in modern cargo systems. These sensors form part of IoT-based systems and used to monitor and track the cargo in real-time. This allow customers, captains and crew members to monitor temperatures, position, and so forth (Larsen, 2020).

- Navigation

  Modern navigation systems extensively make use of GPS, radar, sonar and computerised maps. Information from these systems is used with radio and satellite-based communication systems by navigation officers to navigate ships, especially in the dark and during inclement weather of low visibility (Julius, 2016).

- Environmental compliance

  Modern shipping needs to comply with the ever-increasing environmental regulations towards the UN Sustainable Development Code (SDGs), as such various ICT-related technologies are used to measure, manage and report on environmental-related aspects regarding each vessel. Further, by using cargo, port and environmental data, ships van plan their voyages, take shorter routes and adapt speed to port availability and thereby saving fuel (Moan, 2022).

- Predictive maintenance

  The large amounts of data that is continuously captured can be used for proactive analysis of the state of the ship's machinery or equipment (Marine Digital, 2023). Sensors, robots and smart condition monitoring technologies capture real-time data from equipment, systems and machinery, among other things, about the 'health' and status of the ship (Larsen, 2020). Predictive maintenance is definitely one of the foremost advancements of IoT systems in the modern shipping era.

Thus, the effective use of ICT-based systems contributes, amongst other things, to the delivery of supply chain transparency, assisting with effective navigation, reducing the ecological footprint and minimising the operational costs associated with ship inspections and maintenance. These are just some of the many reasons for the proliferation of data-capturing sensors and many ICT-related systems integrated all-over modern ships and vessels and associated cargo.

"Data is the new gold of the shipping industry" (Larsen, 2019). From this it is clear that quality, well-integrated, data needs to be captured, processed and analysed to be turned into trusted intelligence (Larsen, 2019), that can be used to ensure successful operational, strategic and competitive decisions.

4. Vulnerabilities of ICT and Related Shipping Data

Data becomes 'gold' when it is utilised to gain understanding and strategically integrated into operations and decision-making (Larsen, 2019). To be this valuable, it is logical that data needs to be accurately captured, processed and analysed. Only if this is the case trusted intelligence can stem from this data. Further, this data can only be valuable if it is standardised, accurately and securely distributed, and transmitted between ship and shore. Today it is imperative that reliable, seamless internet connectivity ensures the safe and secure flow of business intelligence (Larsen, 2019). As this process is making use of cyberspace, it is clearly littered with possible vulnerabilities.

The operational technology (OT) of modern ships is increasingly integrated with advanced ICT systems generating data, but also introducing more vulnerabilities to capture quality data. The continual adoption of cloud computing, the IoT and autonomous technologies to interconnect OT and ICT also lead to more cybersecurity risks coming to the fore. Therefore, the maritime industry has become highly vulnerable to cyber-related security risks (Cusimano et al, 2020). As a result of the continued integration of OT, IoT and related ICT systems in the maritime industry, cybersecurity has become very apparent in the industry (Cusimano et al, 2020). IoT devices and resultant systems are not necessarily secure by nature and therefore must be secured.

It is apparent that the maritime industry continues to embrace ICT solutions to become more effective. It is also very clear that this advancement, that depends on quality data, is increasingly exposed and getting vulnerable to cybersecurity risks that are threatening the quality of the data.

5. Cybersecurity in Maritime Industry

Cybersecurity is basically the overall effort to secure the ICT systems, onboard hardware and related sensors, as well as the data involved. This data needs to be protected from data leaks as a result of unauthorised access as well as the illegal manipulation and disruption thereof (Marine Digital, 2022). Cyberattacks on the navigational systems are well documented and usually takes place through the interference with automatic identification systems and electronic maps, the jamming of GPS and the manipulation of shipping management systems. These attacks usually take place by means of the introduction of malware, ransomware software and viruses (Princeton, 2018).

Cybersecurity, which has really become critical lately and should be implemented at all levels of the organisation. The cybersecurity effort should be a collective approach from all parties involved towards the well-being of the ship, its content and those onboard. From senior management onshore to crew members onboard should be involved in this securing process. All these parties and people contribute to the cybersafe culture and thereby ensuring the safe and efficient operation of the ship (Marine Digital, 2022). A brief overview of how cybersecurity and related research has grown in prominence lately will follow as well as an introduction to related cybersecurity vulnerabilities and challenges in the maritime industry.

5.1 The History of Cybersecurity

The rapid progress and adoption of technology in the maritime sector have heightened its susceptibility to cybersecurity risks. In the past decade, various incidents have highlighted vulnerabilities, with infrastructure like maritime vessels, port facilities, and the supply chain being exploited or targeted. Each element within the maritime industry necessitates specific critical operations to safeguard its cybersecurity.

Mawer, et al (2024) examined the historical trajectory of cybersecurity in the maritime sector which revealed a notable surge in cyber threats over the past two decades. While maritime technology has rapidly advanced, the corresponding development of cybersecurity systems has lagged. The integration of modern systems with legacy infrastructure has created additional opportunities for cyber threats. Research in cybersecurity in the maritime industry started to receive more attention, particularly from 2014 onwards. It is, however, seen that the majority of the research originated from the United States, China, the United Kingdom, and Norway.

It has been seen that over the past ten years, there have been numerous cases of infrastructure being targeted or compromised, including maritime vessels, port facilities, and the supply chain. Each facet of the maritime industry demands distinct critical system operations for cybersecurity assurance.

5.2 Cybersecurity Vulnerabilities and Challenges

The maritime industry has grown highly dependable on ICT and related cyberspace over the last decade or so, but also became very vulnerable to cybersecurity threats. This is mainly due to the integration of OT and ICT systems. As a result of the adoption of IoT, cloud computing and autonomous technologies, the integration between OT, ICT systems and the internet will get stronger and resulting in more cybersecurity risks coming to the fore. In fact, cybersecurity-related risks have resulted in cyberattacks that increased by 900% over three years (2018–2020) (Cusimano, 2020; Von Solms, 2023).

Successful cybersecurity attacks, directed on the interconnected OT and ICT environment, can give rise to cybersecurity incidents with detrimental consequences. The following are a few examples of well-documented cybersecurity attacks that have taken place over recent years.

Maersk, the world's largest shipping container transport company, had a cybersecurity attack in July 2017. The resultant damage amounted to US$250–300 million. This ransomware attack resulted in the reinstallation of 45 000 workstations and 4000 server computers worldwide (Princeton, 2018; Von Solms, 2023).

In February 2017 hackers apparently hacked into the navigation system of a German container vessel. This 10-hour long attack was conducted by 'pirates' who totally took over the vessel's navigation system. The idea was apparently to steer the vessel to an area where these 'pirates' could board and take over the ship. The situation was eventually resolved by taking ICT experts on board to regain control of the navigation systems (Marine Digital, 2022; Von Solms, 2023).

During June 2017, at least 20 vessels in the Black Sea reported that their automatic identification systems erroneously indicated their position somewhere 32 km inland. These incidents lead to the risk of GPS spoofing receiving lots more attention, as such spoofing events may lead to disastrous consequences such as ship collisions (Marine Digital, 2022; Von Solms, 2023).

In yet another incident, in July 2017, a British oil tanker steered accidentally into Iranian waters and was seized by Iran. It is believed that false GPS coordinates was fed to the ship (Marine Digital, 2022; Von Solms, 2023).

Cyberspace has changed the way in which the modern world operates, does business, communicates and get entertained. Although slower than other industries, the maritime industry is catching up and harnessing the benefits cyberspace has to offer. The maritime industry has become highly vulnerable to cybersecurity attacks that can lead to disastrous and costly incidents when successful. With the maritime industry, tightly interwoven in cyberspace, it is imperative that dedicated attention is given to related cybersecurity efforts, especially from a management and crew member point of view.

In April 1912, the 'unsinkable', luxurious, technologically advanced Titanic set sail on its maiden voyage and the totally unexpected happened. The Titanic hit an iceberg that ruptured the side of the ship, resulting in the failure of the ultramodern design of watertight compartments and the ship that sank. The lesson from this is never label new and advanced technologies and designs, such as modern ICT-related systems and the usage of cyberspace, as infallible.

6. Cybersecurity as the Cyber-'Iceberg'

It is one thing to adopt the advantages that cyber technology offers, but it is another to face the numerous, continuous and changing associated risks that accompany it. In view of the maritime industry's dependence on cyber technologies for its well-being, it is essential that good governance and due care be applied to manage the associated cyber-related threats, the cyber-'icebergs' that are all but obvious. Such risks include the cyberthreats that exploit certain vulnerabilities in the technological systems, ultimately having a negative impact on the related assets. Typical threats include malware, ransomware, denial of service attacks, phishing attacks, spoofing attacks, among others (Princeton, 2018).

Cyberattacks on modern vessels are constantly happening and resulting in numerous successful attacks, with huge losses incurred as mentioned earlier. Therefore, it has become the norm, as in any industry where cyber technologies are being utilised, for appropriate levels of cybersecurity to be implemented. From a management point of view, it is therefore crucial for the well-being of the vessel, its freight and those onboard to apply adequate cybersecurity measures related to the cyber environment.

Like an iceberg, much of which lies hidden beneath the surface, most cyberthreats are unknown. Real physical icebergs may no longer pose huge risks to the shipping industry, but modern cyber-'icebergs', ever-present in

all 'oceans', need to be approached with caution. Therefore, it can be argued that cybersecurity forms part and parcel of the modern seaworthy certificate. Two parties that form a critical part in countering modern cyberthreats are, firstly, crew members that need to be skilled with data science skills (Larsen, 2020) and management that ensure that due care is exercised to protect themselves against the ever-present cyber-'icebergs'.

6.1 Cybersecurity Education and Awareness

Sound cybersecurity measures to protect on-board ICT systems from being breached by malicious, intentional cyberattacks is one of management's main responsibilities. However, many system security breaches are as a result of the negligence or ignorance of legitimate crew members, owing to a lack of cybersecure skills. Thus, crew members may unintentionally render cybersecurity vulnerable, eventually assisting a successful cyberattack that is obviously detrimental to the vessel, its owner, and the freight and the people on board.

On the evening of 14 April 1912, the 'unsinkable' Titanic hit an iceberg and sank. Word has it that two other ships sent messages to the Titanic warning it about icebergs. Apparently, radio operators were so busy relaying passengers' messages to shore that the warning of a huge iceberg in the vicinity was never conveyed to the bridge. Another radio operator reprimanded another ship for disturbing him as he was busy handling passengers' messages.

It is clear that human error, ignorance and incompetence can, unintentionally assist breaches in system security that may eventually end in a disaster. The case of the Titanic highlights that, ideally a vessel's communication channel(s) should not be used for both operational functions and non-critical, social purposes.

Crew members are generally trained and skilled to conduct one or two specific tasks whilst at sea, most of which generate additional electronic data that is captured, communicated and stored by means of some system; however, these crew members are not usually fully trained or skilled to do so in a cybersecure manner. Therefore, the ignorance or incompetence to securely operate cyber-oriented systems is a huge vulnerability towards cybersecurity and ultimately the vessel. Further, the fact that crew members, when off duty, in many cases use the same communication link between the vessel and the shore for social entertainment, recreation and communication as the vessel uses for critical operation tasks, like navigation, collecting weather information, etc. makes that communication channel prone to cyberattacks. The bottom line is, it is imperative that crew members are all skilled to be properly cybersecurity aware and competent. If not, crew members can form part of the cyber-'iceberg'.

6.2 Governing the Cyber-'Iceberg'

The international Telecommunication Union defines cybersecurity as 'the collection of tools, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, the organisation and the users' assets' (Cusimano, 2020). From this definition it is clear that cybersecurity is a structured process, starting at senior management who is ultimately responsible and accountable for the well-being of the ship, the crew, and the freight (Androjna, et al, 2020).

Most regulatory bodies, industry associations and standards bodies agree that maritime cybersecurity is highly vulnerable and needs to be addressed urgently (Cusimano, 2020). The International Maritime Organization (IMO) adopted resolution MSC 428(98) in 2017 to assist in addressing this need (IMO, 2017b). This resolution states that owner and managers of ships should assess cyber-related risks and introduce relevant measures accordingly across all functions of the vessel's safety management systems (SMS). To assist in this regard, the IMO published Guidelines on Maritime Cyber Risk Management and indicated that the risk management process should start with senior management (IMO, 2017a). Resolution IMO MSC 428(98) calls for senior management and/or administration to control the process to ensure that cyber risks are adequately addressed in their safety management systems (IMO, 2017b). The maritime industry is no different than any enterprise and therefore its cybersecurity environment should be managed and governed like any modern ICT environment. The Control Objectives for Information and Related Technology (COBIT) (COBIT, 2023) and the ISO/IEC 27000 series (IT Governance Institute, 2023) are well-known and generally used in industry for this purpose and therefore these would be of great value in addressing IMO resolution MSC 428(98) (Von Solms, 2023).

COBIT is an industry best practice and predominantly used in the IT management and governance environment (COBIT, 2023). The ISO 27000 family of information security management standards mutually supports

information security management standards (ISO, 2023). These best practices can be used to effectively address the resolution IMO MSC 428(98) (Von Solms, 2023).

7. In Conclusion

This paper highlighted the technological advancement in the maritime industry, especifically over the last few decades. The introduction and integration of sensor technologies, IoT and modern ICT systems with the operational technologies of vessels, have really resulted in modern vessels to be technologically advanced and part and parcel of cyberspace. Also, along with it's involvement with cyberspace, came the vulnerabilities associated with cyber threats. Therefore, cybersecurity to protect and safeguard the shipping industry has become one of the main modern challenges of the industry. This has gain so much attention, that the IMO has made certain resolutions in this regard.

The IMO has stated it clearly that senior management should take control of the management and governance processes to protect against cyber-attacks, as they are ultimately responsible for the well-being of the vessels, the crew and the freight. Further, as most of the crew members work daily with valuable data that gets captured, analysed and transmitted, it is imperative that these members are properly skilled to protect the integrity, confidentiality and availability of this valuable data. If these crew members are not adequately educated, they can unintentionally render the cyber-related systems vulnerable and thereby partake in resultant cyber- attacks. In both cases above, these human parties can be deemed part of modern cyber-'icebergs'.

References

Abi-Saab, C. (2018) The Maritime Industry is slowly embracing technology, but some will be left behind! LinkedIn. Available online: https://www.linkedin.com/pulse/maritime-industry-slowly-embracing-technology-some-left-abi-saab/

Androjna, A., Satler, T. B. and Srše, J. (2020). An overview of maritime cyber security challenges, 20th International Conference on Transportation Science. Available online: (PDF) AN OVERVIEW OF MARITIME CYBER SECURITY CHALLENGES (researchgate.net).

Arreola-Risa, A., Ayala-Solorzano, O., Gonzalez-Rodriguez, M., & Rojo-Alvarez, J. L. (2017). Improving maritime situational awareness by integrating unmanned aerial vehicles and crowdsourcing. Transportation Research Part C: Emerging Technologies, 82, 57-74.

Baldauf, M., Ma, Y., & Zhang, G. (2016). Maritime navigation and safety using electronic chart display and information systems (ECDIS). WMU Journal of Maritime Affairs, 15(1), 33-56.

COBIT (2023) Control Objectives for Information Technologies. ISACA, Available online: www.isaca.org.

Cusimano, J., Ayala, M. and Villano, G. (2020) Navigating cybersecurity challenges in maritime operational technology. Available online: https://maritime-executive.com/editorials/navigating-cybersecurity-challenges-in-maritime-operational-technology.

Hegland, T. J., Nguyen, H. Q., Choo, K. K. R., & Hegarty, C. J. (2017). Radar technology in maritime navigation. In OCEANS 2017 - Aberdeen (pp. 1-6). IEEE.

Hui, K. S., Pang, W. M., Yang, L., & Yu, D. (2019). Maritime safety enhancement based on an automatic identification system using a deep learning technique. Safety Science, 115, 243-255.

IMO (2017a). Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ. 3, June.

IMO (2017b). Maritime Cyber Risk Management in Safety Management System, Resolution MSC 428(98), adopted June 16.

ISO (2023). ISO/IEC 27000 series, International Standards Organisation. Available online: www.iso.org.

IT Governance Institute (2023). What is COBIT 5: Definition and explanation. Available online: What is COBIT 5? Definition & Explanation (itgovernance.co.uk).

Julius, P. Apud (2016) Information technology applications in the maritime industry. Available online: Information Technology Applications in the Maritime Industry – The Maritime Review.

Kaplan, E. D., & Hegarty, C. J. (2006) Understanding GPS: Principles and Applications. Artech House.

Kundu, A. (2023) Ship Propulsion Through The Ages: An Overview, Shipfinex. Available online: https://www.shipfinex.com/blog/ship-propulsion#:~:text=Before%20the%2019th%20century%20ushered,galleys%20with%20oars%20took%20precedence.

Larsen, R. (2019) What's the value of maritime-specific software? Available online: What's the value of maritime-specific software? (dualog.com).

Larsen, R. (2020) How ICT solutions can be used strategically in shipping. Available online: https://www.dualog.com/blog/how-ict-solutions-can-be-used-strategically-in-shipping.

Lind-Olsen, M. (2019) ICT solutions bring ship and shore close. Available online: https://www.dualog.com/blog/ict-solutions-bring-ship-and-shore-closer.

Maritime Cyprus (2020) The evolution of ship propulsion, Maritime Cyprus. Available online: https://maritimecyprus.com/2020/03/12/infographic-the-evolution-of-ship-propulsion/

Marine Digital (2022) The importance of cybersecurity in the maritime industry. Available online: https://marine-digital.com/article_importance_of_cybersecurity.

Marine Digital (2023) Predictive Maintenance for Marine Vessels. Available online: https://marine-digital.com/article_predictive_maintenance_for_marine_vessels#:~:text=Maintenance%20prediction%20is%20a%20proactive%20approach%20to%20dealing,that%20is%20strictly%20adhered%20to%20on%20board%20ships.

Matuszak, J. (2021) 8 Technology Trends Transforming the Maritime Industry, KnowHow – Defence, Aerospace and Marine, IT and Digital. Available Online: https://knowhow.distrelec.com/defence-aerospace-and-marine/8-technology-trends-transforming-the-maritime-industry/

Mawer, T., Von Solms, S. & Meyer, J. (2024) Identifying the Scope of Cybersecurity Research Conducted in the Maritime Industry: 2003 – 2023. Accepted for publication: ICCWS 2024.

Moan, S. (2022) The value of ICT in the maritime industry. Available online: The value of ICT in the maritime industry (dualog.com).

Moussavi, R., Boroushaki, M., & Khorasani, K. (2020) Artificial intelligence in maritime navigation: Challenges and opportunities. Ocean Engineering, 204, 107336.

Princeton, P. (2018) Top 4 Trending Technologies in the Maritime Industry, Patrick Princeton. Available online: https://www.searates.com/blog/post/it-technologies-in-the-marine-industry.

Rao, A. S. (2019) Satellite communication in the maritime sector: A review. Journal of Navigation and Port Research, 43(3), 245-255.

Saeed, M., Tang, Y., Naik, K., & Choo, K. K. R. (2021) Biometric technologies for maritime security: A comprehensive review. Ocean Engineering, 225, 108953.

Smith, J. R. (2018) Maritime communication: Past, present, and future. Journal of Maritime Research, 15(2), 45-58.

Sun, Z., Zhang, D., Zhang, G., & Li, S. (2020) Cyber-physical systems in maritime: A comprehensive review. Journal of Marine Science and Engineering, 8(11), 898.

Voyager (2023) Embracing Digitalization in the Maritime Industry. Voyager. Available online: https://www.voyagerportal.com/digitalization-in-maritime/

Wang, C., Li, X., & Zhang, Y. (2020) Integration of IoT and cloud computing for smart maritime logistics. IEEE Access, 8, 118740-118752.

Yang, L., Ren, L., & Ji, J. (2021) Smart shipping: A comprehensive review. Transportation Research Part C: Emerging Technologies, 128, 103030.