【欧州】【海事】

Maritime Issues – Cyber security: Maritime Issues: Cyber security in maritime transport and the question of cyber security measures for autonomous ships

Andrea Antolini　Former Researcher JTTRI

【概要：Summary】

All means of transport including vessels are undergoing an accelerated development towards automation. The shipping industry's main goal regarding the introduction of Maritime Autonomous Surface Ships (MASS) is to eliminate the requirement of having a human crew on board of the vessels at all times. Remotely controlled and autonomous ships are expected to be safer, more efficient, and cheaper to run than manned ships. However, they have an even higher need for taking measures that guarantee cyber security than traditional vessels. Cyber security is a main concern for in the entire transport sector as there have been observed an increasing number of incidents of cyber attacks. Cyber security is also concerning the maritime sector, which is also a potential target of cyber attacks.

A very large proportion of cyber security incidents are caused by basic errors when using computers and the internet. In addition, ships can be attacked through data connections with the land-based services. Therefore, the increased connectivity of modern ships to on-shore via networks makes on-board systems especially vulnerable to cyber attacks. In order to prevent unauthorized access or cyber attacks, ship operators must take measures for increasing their ships' cyber safety and security.

The cyber security awareness in maritime transport and vessel operation is even more vital when considering the introduction of remotely controlled and fully autonomous, unmanned ships in maritime transport. Currently, the International Maritime Organisation (IMO) reviews all legislation important for the utilisation of autonomous ships of all grades of autonomy. All legislation needs to be considered, but the IMO's work on reviewing legislation regarding autonomous ships is conducted without any deadline. The review of legislation is taking time and cyber-specific amendments to the International Ship and Port Facility Security Code (ISPS) and the International Security Management Code (ISM) will only come into force on 1 January 2021, including the obligation of introducing risk management processes. Therefore, it still could take years until rules for cyber security, especially for autonomous ships, are introduced.

Regarding the cyber security of autonomous ships, there is strong need for considering the aspects of protecting the autonomous ships' data streams and the IT systems from cyber attacks as they are the fundamental basis of their operational readiness. Therefore, cyber security aspects in remotely controlled or fully autonomous ships will have to be attentively considered. In case of autonomous ships, cyber security solutions should be the result of a holistic approach, encompassing technology, people and processes.

【記事：Article】

1. Autonomous ships and the set up of international legislation

In recent years, the development of autonomous shipping has accelerated and Maritime Autonomous Surface Ships (MASS) are seen as a key element for a competitive and sustainable future shipping industry. Remotely controlled and autonomous ships have the potential to redefine the maritime industry. They are expected to be safer, more efficient, and cheaper to run than manned ships. They are also considered being able to reduce the risk of human errors. In Europe, in particular Norway is supporting the development of MASS operations and Norway has already dedicated some sea areas for MASS testing. The 80 m long Yara Birkeland autonomous container ship is due to be launched in 2019 and following trials with a small crew on board, it will be operating autonomously by 2020. The autonomous container ship is planned to sail between Yara's Norwegian production facilities at Herøya and the ports of Brevik and Larvik in Norway. Furthermore, in April 2019, Wilhelmsen and KONGSBERG established the first autonomous shipping company named "Massterly".

These trials with autonomous vessels are taking place at national level, and they only need approval by national regulators for their operation. Instead, for international maritime transport, crewless MASS ships will need to comply with international legislation of maritime transport, based on current practices for safe navigation. To integrate autonomous ships into the legislation of international maritime transport, existing regulations need to be revised for taking account of the new remotely controlled ship technology.

Regarding the introduction of legislation on autonomous vessels in international maritime transport, the 98th IMO's Maritime Safety Committee (MSC) recognized that the IMO should take a proactive and leading role in determining the safe, secure and environmentally sound operation of MASS. The MSC 99 established a correspondence group to test the framework of the regulatory scoping exercise on MASS, including the set up of preliminary definitions of MASS and their degrees of autonomy. The IMO's MSC 100 approved the framework and methodology for the regulatory scoping exercise on MASS. Each instrument related to maritime safety and security, and for each degree of autonomy, provisions will be identified. The degrees of autonomy include several levels, including remotely controlled ships with seafarers or without seafarers on board as well as fully autonomous ships, which are able to make decisions and determine actions by itself.

The MSC 101 made progress on the scoping exercise to develop a regulatory overview on the necessary revisions to establish a safe, secure and environmentally sound operation of MASS within the IMO instruments. The MSC also decided on further aspects of the utilisation of autonomous ships and developed a framework for analysing applicable IMO regulations and the possible gaps between current regulations and the technological development. The first step is to identify in treaties and provisions those rules, which apply to MASS or which could prevent MASS operations. Once the first step is completed, a second step will be to analyse and determine the most appropriate way of addressing MASS operations. The shipping industry considers it as important that regulations are getting adjusted for the autonomous ships' technology in order to avoid a hindrance to further advances in this technology. Regulations should also be made more flexible to allow for a support of the development of autonomous ships. A delay in the revision of international legislation at IMO level could well lead to a situation in which MASS will already operate in national waters before the international regulations have been revised. Therefore, regulators will need to move quicker in their revision work because the technology is advancing rapidly and ship owners will want to have clarity on the regulation before investing in the technology. More national authorities could approve MASS operations in national waters, but it will need the IMO to adapt the international regulation instruments for the introduction of MASS.

2. The cyber security considerations for international maritime transport

2.1. Digital technologies change ship handling

The increasing use of digital technologies in the management of vessels has also made them more vulnerable against cyber attacks. As the number of reported cyber attacks affecting the shipping industry continues to rise. After a cyber attack on A.P. Moller-Maersk in summer 2017, which delayed the entire fleet, cyber crime has become a much higher threat to Danish shipping companies alongside piracy and other forms of crime. Vulnerabilities in shipping show how far the industry has to improve for proper cyber security. However, the maritime transport industry has been rather slow to realise that ships are now part of cyberspace. Also the International Maritime Organisation (IMO) has been late in considering appropriate regulations when it comes to cybersecurity. In 2016, the IMO issued its interim cybersecurity risk management guidelines, which are broad and not particularly maritime specific. In 2017, the IMO amended two of its general security management codes to include cybersecurity. The International Ship and Port Facility Security Code (ISPS) and the International Security Management Code (ISM) detail how port and ship operators should conduct risk management processes. Making cybersecurity an integral part of these processes should ensure that operators are at least conscious of cyber-risks and this could lead to a more holistic approach to a maritime cybersecurity regulation. However, both cyber-specific amendments to the ISM and ISPS will only come into force on 1 January 2021, and they only represent the beginning of necessary measures.

There is an increasing need for maritime companies to pay as much attention to their onshore business networks, as they do to their offshore assets. This is an important consideration for traditional vessels but even more so for autonomous ships. While autonomy offers a solution to many issues facing the maritime industry, cybersecurity and countering cyber attacks are the key challenges for the utilisation of autonomous ships. The digitalization of the transport system makes transport also more vulnerable to cyber risks and accordingly, cyber security is a subject of importance also for maritime transport and in particular for autonomous vessels. However, the fact that shipping connectivity and the introduction of digital technologies is a relatively recent development means that some operators and owners in the maritime sector are still lagging behind in taking measures regarding cyber security. Moreover, the distinction between information technology and operational technology systems on board of vessels need to be considered. Information technology systems are used to create, store and transfer data as information, whereas operational technology systems are used to control or monitor physical processes. When operational and/or information technology vulnerabilities are exposed or exploited, there can be implications for safety, particularly where critical systems like bridge navigation or main propulsion systems.

2.2. Cyber security for maritime transport and particular challenges for remotely controlled autonomous ships

Cyber attacks could pose an increasing security threat to the about 50,000 operating ships, but there are several core issues that make cybersecurity for the maritime industry particularly challenging. Firstly, there are many different classes of vessels, all of which operate in very different environments. These vessels have different computer systems and many of these systems are built to last over 30 years, which implies that many ships run out-dated and unsupported operating systems, highly vulnerable to cyber attacks. Secondly, the ship crews using these systems are highly dynamic, often changing at short notice. As a result, crew members are often using systems they are unfamiliar with, and thereby increase the potential for cyber security incidents relating to human error. The maintenance of on-board systems, including navigational ones, is often contracted to a variety of third parties. A third complexity is the linkage between on-board and terrestrial systems. Many maritime companies stay in constant communication with their vessels and therefore, the cyber security of the ship is also dependent on the cyber security of the land-based infrastructure.

The remote and autonomous ships will pose an extra difficulty to cyber security of systems on board and at land, if those ships intend to reach at least the same security level of existing modern vessels.

Traditionally a ship's Operation Technology (OT) and its Information Technology (IT) are divided and different areas. However, in case of fully connected, remotely controlled ships or fully autonomous ships, the OT and IT are fully connected, if the ship is remotely controlled by land-based services. In this case, a malfunctioning IT may lead to a significant disruption of the operation of OT systems, which would affect the entire operational readiness of the ship. It could lead to significant delay of a ship's operation or could cause harm to people or the marine environment. Accordingly, since remotely controlled and autonomous ships need to communicate in real time in order to navigate to its destination, avoid collisions along the way, and perform complex manoeuvres, such as docking, the autonomous ships need an even superior safety and security assessment to prevent any cyber attack or malicious interruption of their communication network.

Considering the general delay in the review of the IMO's legislation regarding the remote and autonomous ships, there is not existing any legislative basis for cyber security of remote and autonomous ships, also because the shipping industry has to integrate the cyber security rules into their Safety Management Systems, SMS only by 1 January 2021, not to mention any regulation of cyber security for remotely controlled or autonomous and unmanned ships.

2.3. Measures to manage cyber risks

Cyber threats may arise from malicious actions like hacking, the introduction of malware or the unintended consequences of benign actions like software maintenance or user permissions. In general, these actions expose vulnerabilities, which can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber discipline. Therefore, cyber risk management needs to consider both kinds of cyber threats, malicious action as well as unintended consequences of benign actions. Consequently, it is imperative for every shipping company to take measures to provide cyber security for their vessels in general. However, it is of fundamental importance in case of remotely controlled or fully autonomous ships.

In June 2017, the IMO's Maritime Safety Committee (MSC) adopted Resolution MSC.428(98) incorporating Maritime Cyber Risk Management into the ISM Code in order to raise the profile and importance of protecting ships, crews and cargos from the threats of accidental cyber-related incidents and cyber attacks. On 5 July 2017, the IMO published the "Guidelines on Maritime Cyber Risk Management" in addition to the resolution on Maritime Cyber Risk Management in Safety Management Systems adopted by the MSC. The IMO's "Guidelines on Maritime Cyber Risk Management" laid down in MSC-FAL.1/Circ.3 and MSC.1/Circ.1526, provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The companies are advised to consult the Resolution MSC.428(98) and identify possible cyber risks with regard to their operations ashore and aboard. The Resolution states that cyber risk management should be conducted with regard to objectives and requirements of International Safety Management Code. The identification, analysis, assessment and communication of cyber related risks, as well as suggestions of mitigation measures, is recommended. The cyber risks should be appropriately addressed in the Safety Management Systems (SMS) no later than the first annual verification of the Document of Compliance (DOC) after 1st January 2021. Ship owners risk having ships detained if they have not included cyber security in the ISM Code safety management on ships by 1 January 2021. Thereby, the IMO has taken the decision to incorporate mandatory cybersecurity requirements into the International Safety Management Code ISM. However, there is no mentioning of the autonomous ships or MASS.

2.4. Cyber risk assessment and management

Cyber risk management needs, firstly, to identify the roles and responsibilities of users, key personnel, and management both ashore and on board of ships. It needs to identify the systems, assets, data and capabilities, which, if disrupted, could pose risks to the ship's operations and safety. In case of autonomous ships, this would greatly vary, depending on the grade of autonomy and whether it is a remotely controlled ship with seafarers or without seafarers on board or a fully autonomous ship.

The risk assessment process for cyber threats starts by assessing the systems on board of a ship, in order to map their robustness to handle the current level of cyber threats. The assessment includes the identification and evaluation of key ship operations on board that are vulnerable to cyber attacks, and the likelihood of their occurrence, which influences the establishment and the priorities of protection measures. This includes also human factors, and the policies and procedures related to the use of these systems. The risk assessment should physically test and assess the IT and OT systems on board. This includes the identification of existing technical and procedural controls to protect the on-board IT and OT systems and their specific vulnerabilities.

Protecting the autonomous ships' but also traditional ships' data streams and the IT systems would be crucial as well as considering potential sources of threats and vulnerabilities and associated risk mitigation strategies. A number of potential control options for cyber risk management should be taken into consideration, including management, operational or procedural, and technical controls, among others.

Technical measures to protect the vessels against cyber incidents need to be implemented and the continuity of operations needs to be ensured. This may include configuration of networks, access control to networks and systems, communication and boundary defence and the use of protection and detection software. Activities and plans need to be implemented to provide resilience against cyber incidents. This may include training and awareness, software maintenance, remote and local access, access privileges, use of removable media and equipment disposal.

The International Association of Classification Societies (IACS) announced to establish a joint cyber risk management-working group. It also utilises the shipping industry Guidelines on Cyber Security, ISO/IEC 27001 and the US National Institute of Standards and Technology's Framework for Improving Critical National Infrastructure Security (the NIST Framework). Also the International Organisation for Standards (ISO) has established a working group of specialists to draft a maritime cyber risk management standard to develop a more robust and broad based maritime cyber risk management strategy. The ISO/IEC 27001 standard on Information technology - Security techniques - Information security management systems - Requirements was published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

2.5. BIMCO Guidelines

In January 2015, BIMCO launched the set of guidelines to help the global shipping industry to preventing problems resulting form a cyber incident on-board of a ship. The aim was to provide the shipping industry with clear and comprehensive information on cyber security risks to enable ship owners to take measures to protect against attacks and to deal with the eventuality of cyber incidents. BIMCO together with CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI published the second edition of detailed guidance on cyber risk management for ship owners and operators in the "The Guidelines on Cyber Security Onboard Ships" in July 2017. The aim of these guidelines is to provide practical recommendations on cyber security and safety in order to deal with the emerging cyber security threat to vessels and vessel operators. This second edition includes information on insurance issues and how to effectively segregate networks, as well as new practical advice on managing the ship to shore interface, and how to handle cyber security during port calls and when communicating with the shore side. The Guidelines have also been aligned with the recommendations given in the IMO's Guidelines on cyber risk management, which were adopted in June 2017.

However, with cyber threats constantly evolving, BIMCO along with several maritime industry organisations published the third version of the "Guidelines on Cyber Security onboard Ships. Version 3" in December 2018. This third edition of cyber risk management guidelines has addressed the requirement to incorporate cyber risks in the ship's safety management system (SMS). The new edition also includes experience with risk assessments of operational technology (OT) such as navigational systems and engine controls, and provides more guidance for dealing with the cyber risks to the ship arising from parties in the supply chain. This new edition provides more information to assist shipping companies conduct proper risk assessments and improve their safety management systems to protect ships from cyber-incidents, including measures that all companies should consider implementing to address cyber risk management in an approved Safety Management System (SMS). The new guidelines consider risk assessments of operational technology (OT) including navigational systems and engine controls. In order to mitigate the dangers of cyber security incidents affecting the Operational technology (OT) risks, the guidelines reflect on the increased connection of OT with integrated Information technology (IT), which, if connected to the internet, could cause malfunctioning of IT or OT. However, an inoperative OT could pose a real risk of harm to people, the ship or the marine environment. The guidelines provide guidance to ship owners and operators on how to assess their operations and establish procedures to enhance cyber resilience on board their vessels. Considering the risk of malware infecting a ship's systems through the many parties associated with the operation of a ship and its systems, the guidelines include evaluating the security of service providers, providing a minimum set of requirements to manage supply chain or third-party risks and ensuring that agreements on cyber risks are formal and written. The guidelines also emphasize the need for ships to be able to disconnect quickly and effectively from shore-based networks, if required.

The BIMCO guidelines point out that it is important to protect critical systems and data with multiple layers of protection measures, which take into account the role of personnel, procedures and technology. Finally, BIMCO recommended IMO to give the same importance to the cyber threats than to any other.

3. Steps to improve cyber security on-board of ships

When considering the needs to assess cyber risks arising from the use of IT and OT on-board ships and choosing the appropriate safeguards against cyber incidents, the ship operator and owner has to consider several steps in the line to achieve cyber security. When considering the cyber risks related to the utilisation of the IT and OT on board of a ship, the Safety Management System should include instructions and procedures to ensure the safe operation of ships and protection of the environment in compliance with relevant international and flag state legislation.

According to Wärtsilä, a major marine engine manufacturer, the vast majority of cyber security attacks are conducted by means of phishing and social engineering techniques, but most actual breaches of security can be attributed to human error. Wärtsilä's strategy for detecting and mitigating cybersecurity attacks is based on training and awareness programs for all personnel.

In September 2017, Inmarsat presented its new cyber resilience service Fleet Secure service to detect vulnerabilities, respond to threats and protect ships from cyber attacks. The cyber risk monitoring service Fleet Secure gives shipping operators and managers the tools they need to protect their fleet from cyber attack, detect vulnerabilities, and respond to threats. It also protects the vessel networks from intrusion via infected USB sticks and crew devices. Inmarsat's Fleet Secure service detects external attacks via high-speed satellite broadband,

In order to improve the maritime cyber security, also DNV GL registrar and classification society intends to offer solutions addressing systems, software, procedures and human factors, using a systematic approach to assess the cyber security of vessels and their interaction with land-based management. According to DNV GL, proven cyber security management approaches look at raising the awareness of all stakeholders, including onshore personnel and offshore crews. They assess and implement defensive and reactive countermeasures, and they monitor and review effectiveness and robustness of barriers. DNV GL addresses information technology (IT) as well as the industry-specific operational technology (OT) systems and recommend practice for cyber security resilience management for ships and mobile offshore units in operation. It guides owners, managers and operators of ships or mobile offshore units towards enhanced cyber security of their assets.

The International Marine Contractors Association, IMCA, which represents the offshore support and construction (vessels) industry worldwide has also updated its advice on cyber threats. IMCA's recommended cyber security measures include 20 controls, and sub-controls, that focus on various technical measures and activities with the aim to prioritising defence against the current most common and most damaging forms of attack on IT systems and networks. The IMCA's 20 controls for offshore cybersecurity include the inventory of authorised and unauthorised devices and software actively managed to secure configurations for hardware and software on mobile devices, etc., to continuously assess vulnerabilities and remediate them. Further control includes malware defences, application software security, wireless access control, data recovery capability, security skills assessment and appropriate training to fill gaps in cyber security.

4. Considering cyber security measures for remotely controlled autonomous ships

The maritime industry is still lagging behind other transport sectors regarding the introduction of cyber security measures and terms. Another concerning aspect is the under-reporting of cyber attacks, which seems to be a serious challenge in the maritime industry and for insurers and reinsurance. As a result of this under-reporting of cyber incidents, ship managers might underestimate the likelihood of a cyber attack, according to Furness-Smith. It is a lack of reporting that is providing a false sense of security within the maritime industry. Therefore, ship operators, owners and managers should approach cyber security as an integral part of their overall safety management. In 2017 the IMO issued a set of guidelines on maritime cyber risk management to safeguard shipping from existing and emerging cyber threats and vulnerabilities. The maritime cyber risk management needs to be appropriately addressed in existing safety management systems by no later than 1 January 2021.

However, cyber attacks could still pose an increasing security threat to ships and in future, and to an even higher extent to remotely controlled and fully autonomous ships, as their operational system is fully relying on the IT and remote connections. However, in any case and regardless the exact level and form of autonomy of a ship, cyber security is a serious issue for autonomous ships, because they have an increased dependence on ICT for ship control. On the other hand, autonomous ships' OT and IT systems architecture and operations have not been defined in full detail and the particular potential of cyber threats and cyber attacks for autonomous ships have not been identified, yet.

In their paper, Kavallieratos, Katsikas and Gkioulos identify and categorise the autonomous ships' systems, and they analyse their cyber security. The results are intended to support ship designers and industry to improving the autonomous ship system architecture in order to make ship operations more secure.

The starting point for developing a framework for securing the autonomous ships in future is the assessment of the cyber risks, which they will face. In case of autonomous ships, it is important to examine together security, safety and resilience aspects. In his paper "Cyber Security of the Autonomous Ship", Katsikas points out that although methods for assessing security and safety risks do exist, they have been tailored-made to specific systems like railways or nuclear power plants, but not for autonomous ships. Katsikas states that the level of autonomy of a ship affects also the system architecture. This is a central element in the analysis of the cyber security issues involved with autonomous ships. Therefore, it is not possible to discuss such issues in detail without specifying the exact system architecture in question. Katsikas emphasises that the autonomous ship interacts heavily with its environment and with humans and therefore, effective cyber security solutions should come as the result of a holistic approach, encompassing technology, people and processes.

The maritime industry will have to urgently consider the cyber security aspects of their ships and decisive steps towards cyber attack prevention and resilience will have to be introduced swiftly in case of manned ships, but even more urgently in case of remotely controlled or fully autonomous ships in order to avoid possible cyber attacks.

References:

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL: THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS. In: https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16&sfvrsn=16, retrieved 10 Sept. 2019

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL:The Guidelines on Cyber Security Onboard Ships Version 3. In: https://safety4sea.com/wp-content/uploads/2018/12/BIMCO-Guidelines-on-cyber-security-onboard-ships-2018_12.pdf, retrieved 11 Sept. 2019

DNVGL: Maritime cyber security services and solutions. In: https://www.dnvgl.com/services/maritime-cyber-security-services-and-solutions-73927, retrieved 10 Sept 2019

Furness-Smith, Georgie: Maritime industry must open up about cyber crime. In: https://lloydslist.maritimeintelligence.informa.com/LL1128745/Maritime-industry-must-open-up-about-cyber-crime, 12 Aug 2019, retrieved 10 Sept. 2019

Guidelines on maritime cyber risk management. In: https://safety4sea.com/guidelines-on-maritime-cyber-risk-management/, retrieved 10 Sept. 2019

Guidelines on Maritime Cyber Risk Management. Practices for implementation. In: https://maritimecyprus.files.wordpress.com/2018/11/dromon-guidelines-on-maritime-cyber-risk-management.pdf, OCTOBER 2018, retrieved 10 Sept. 2019

IMO: THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS. In: http://www.imo.org/en/OurWork/Facilitation/Electronic%20Business/Documents/guidelines-on-cyber-security-onboard-ships.pdf, retrieved 9 Sept. 2019

IMO: GUIDELINES ON MARITIME CYBER RISK MANAGEMENT, MSC-FAL.1/Circ.3, 5July 2017 in: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf, retrieved 10 Sept. 2019

IMO MSC: RESOLUTION MSC.428(98) (adopted on 16 June 2017) MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS. In: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf, retrieved 10 Sept 2019

Inmarsat: Inmarsat Maritime unveils 'Fleet Secure' a managed service to power cyber resilience at sea. In: https://www.inmarsat.com/press-release/inmarsat-maritime-unveils-fleet-secure-managed-service-power-cyber-resilience-sea/, 13 September 2017

Katsikas, Sokratis: Cyber Security of the Autonomous Ship. In: http://library.usc.edu.ph/ACM/SIGSAC%202017/cpss/p55.pdf, retrieved 10 Sept. 2019

Kavallieratos, Georgios/Katsikas, Sokratis/Gkioulos, Vasileios: Cyber-Attacks Against the Autonomous Ship: Methods and Protocols. In: https://www.researchgate.net/publication/330756917_Cyber-Attacks_Against_the_Autonomous_Ship_Methods_and_Protocols, January 2019, retrieved 9 Sept. 2019

KPMG: Detect and address cyber risks in the maritime industry. In: https://home.kpmg/no/nb/home/campaigns/2018/10/how-to-detect-and-address-cyber-risks-in-the-maritime-industry.html, retrieved 10 Sept 2019

Maritime industry publishes updated guidelines for cyber security on ships. In: 10/12/18 https://safety4sea.com/maritime-industry-updates-guidelines-for-cyber-security-on-ships/, 10 Sept. 2019

Martin, Keith/ Hopcraft, Rory: 50,000 ships worldwide are vulnerable to cyberattacks. In: https://www.independent.co.uk/life-style/gadgets-and-tech/ships-cyberattacks-vulnerable-worldwide-a8404191.html, 20 June 2018, retrieved 10 Sept. 2019

The future of Maritime Cybersecurity. In: https://securestatecyber.com/cyberbloggen-en/the-future-of-maritime-cybersecurity/, April 15, 2019, retrieved 10 Sept. 2019