Maritime Technology and Research

https://so04.tci-thaijo.org/index.php/MTR

Research Article

Discussing cybersecurity in maritime transportation

Antoni Bielawski and Agnieszka Lazarowska*

Department of Ship Automation, Gdynia Maritime University, 81-225 Gdynia, Poland

Article information

Received: July 11, 2021
Revised: August 13, 2021
Accepted: August 16, 2021

Keywords
Automation,
Autonomous ships,
Maritime cybersecurity,
Piracy

Abstract

The increasing expansion of Operational Technology (OT) and the digitalization of Information Technology (IT) in maritime transportation, as well as the equipping of ships with more automation, despite many benefits, introduces numerous cyber risks, especially with unauthorized access to data and ship systems. Due to the above, it becomes important to raise awareness and take measures to ensure adequate security; this is also important at the level of the virtual securing of ships. This article consists of an introduction to the topic. It presents the current trends and directions of development of maritime transportation and the risks related to them. It contains an overview of the current safety systems on ships and the present safety resolutions. Then, it describes issues related to modern piracy and the weaknesses of ship systems most vulnerable to cyber-attacks.

1. Introduction

According to the United Nations Conference on Trade and Development (UNCTAD) statistics, maritime transportation accounts for approximately 80 % of global trade (UNCTAD, 2020), which, in most of the more developed countries, it exceeds 80 %.

The future is now focused on increasing the automation of ships, which in turn will contribute to their autonomy (Felski & Zwolak, 2020). While technological limitations are no longer a problem, because all the factors to create an independent, fully autonomous vessel exist, legal regulations for, and the safety of, such units have turned out to be problems (Mingyu et al., 2020; Yoo & Park, 2021).

In relation to autonomous vessel implementation, safety and security are among the most important aspects that have been analyzed in recent projects and reports. Safety is regarded in terms of a vessel's capacity to avoid collisions and other incidents, such as foundering, engine and other systems breakdown, or fire and explosion. Security is related to the risks of cyber-attacks and pirates so, under this notion, techniques and processes in regard to crime prevention are considered. Safety and security may be distinguished in terms of motivation, where safety is aimed at the protection of life, health, and the natural environment from any damage the system may cause and is focused on unintentional events. Meanwhile, security is aimed at the protection of the confidentiality, integrity, and availability of information, and is focused on threats coming from

* *Corresponding author: Department of Ship Automation, Gdynia Maritime University, 81-225 Gdynia, Poland*
E-mail address: a.lazarowska@we.umg.edu.pl

outside of the system. These are intentional threats, caused by malicious parties. The differences between safety and security are described in detail in Line et al. (2006).

In a very general way, an offense committed electronically is called cybercrime. In other words, a cybercrime is an offence relating to computer information; it can be defined as a criminal act, where the computer information is the target. Many studies on the definition of cybercrimes have been reported in recent years. According to Xingan (2008), cybercrimes are criminal offences committed by netizens in cyberspace. Other comprehensive approaches to the topic of the definition of cybercrimes can be found in Sabillon et al. (2016) and UNODC (2013).

Techniques, processes, and practices aimed at the protection of networks, devices, programs, and data from cyber-attacks, damage, or unauthorized access are defined as cybersecurity (IMO, 2021a). An example of a project dedicated to the analysis of safety and security aspects of unmanned and autonomous ships is the Maritime Unmanned Navigation through Intelligence in Networks (MUNIN) project (MUNIN, 2015).

In this paper the main aspects of cybersecurity in maritime transportation are presented and discussed. The aim of this paper is to provide introductory information concerning the current state of ship systems and trends in relation to cybersecurity, particularly in relation to unmanned and fully autonomous ships. The rest of the paper is organized as follows. In section 2, recent trends in the development of ships are defined and briefly described, with an emphasis on cyber risks concerning their implementation. Section 3 introduces and briefly describes the most important safety systems applied on ships nowadays. Section 4 concisely describes current rules and regulations in which the concept of cybersecurity has also been implemented. In section 5, current problems and proposals of solutions concerning piracy and cybersecurity are underlined. Section 6 presents the conclusions from the analysis of the AIS, GPS, and ECDIS systems, in terms of their vulnerability to cyber-attacks. Section 7 summarizes the paper.

2. Maritime transportation development trends and potential problems

By 2030, the following maritime transportation innovations are expected to be implemented in the following areas (Lloyd's Register, QinetiQ & University of Southampton, 2015):

- Big Data analysis and wireless communication,
- Power supply and the propulsion of ships,
- Smart ships and autonomy.

These innovations are followed by threats that are increasingly turning into virtual-type threats, popularly known as cyber-attacks.

2.1 Big Data

Big Data is data that cannot be processed in a traditional way. To illustrate the scale of the problem, one can use the statistics that in 2020 the amount of data in the world increased by 4,300 % (Lloyd's Register, QinetiQ & University of Southampton, 2015). Taylor-Sakry defines Big Data as "large sets of complex data, both structured and unstructured which traditional processing techniques and/ or algorithms are unable to operate on" (Jović et al., 2019). In the future, the amount of data will increase year by year; therefore, the management and analysis of big data will become very important. Big Data can be characterized by 3 "V", for "volume", "velocity", and "variety" (Sivan et al., 2014). Sometimes, Big Data is characterized by 5 "V", by adding the characteristics of "veracity" and "value" (Özköse et al., 2015). In maritime transport, the amount of data is constantly growing, and the source of this large amount of information for analysis will be:

- Meteorological and oceanographic data - weather routing,
- Cargo data - quantity, parameter monitoring,
- Navigation and communication - logistics, voyage planning, positioning,

- Maintenance and inspection data - power and fuel management, reduction of CO_2 and NO_x, SO_x emission.

Due to the fact that a lot of information will be transmitted wirelessly in the future, such systems should be adequately protected against potential attacks, such as signal interference, viruses, or cyber piracy. However, wireless information exchange always carries the risk of data interception or a cyber-attack. Therefore, the implementation of Big Data technologies in the maritime market will also increase the risk of, and increase the possible damage caused by, cyber-attacks (Jović et al., 2019). "According to CyberKeel, a Danish cyber security firm, more than 90 % of the largest container lines are vulnerable to hackers" (Trelleborg Marine Systems, 2018).

Kongsberg has created Information Management System (K-IMS), a platform for managing and interpreting Big Data coming from vessels and for remote services. The idea of this system is shown in **Figure 1**. It is worth mentioning that the system also includes Malware Protection, a special device used to scan USB devices connected to the ship's computers. USB devices will not be read by ship computers until they are scanned by the Malware Protection device.

Figure 1 Overview of Kongsberg Information Management System (K-IMS).
Source: Kongsberg Maritime (2015).

2.2 Maritime autonomous surface ships

Fully autonomous ships appear under the abbreviation MASS, which means Maritime Autonomous Surface Ship. By 2022, the project of an autonomous ship called YARA Birkeland is planned to be completed, and will replace the land transport of YARA fertilizers, thereby shortening the route from the main factory to the port of Larvik from 26 km by land to 14 km by sea. The Norwegian company YARA (a producer of fertilizers), wanting to reduce CO_2 and NO_x emissions and, above all, costs, decided to order this autonomous ship. Annually, the company will reduce the number of trucks running between the factory and the port from which the goods are exported by 40,000. The YARA project was created by the Kongsberg company (**Figure 2**). The autonomous ship will be able to transport 120 TEU of cargo, which will also be autonomously loaded through a specially adapted shore infrastructure. The propulsion of the ship will be entirely electric, consisting

of two azimuth thrusters and two bow thrusters, which eliminates the need for a traditional rudder. Power will be supplied from batteries with a capacity of 7 - 9 MWh.

Figure 2 YARA Birkeland.
Source: Kongsberg (2017).

Following the YARA project, other leaders on the market have taken steps to create autonomous ships, including Rolls-Royce, Deltamarin, Inmarsat, and DNC, and have defined the following steps in the development of MASS design. By 2025, it is planned that unmanned ships will be introduced in coastal shipping. By 2030, remotely operated unmanned ocean vessels will be introduced, and by 2035, remote ocean vessels will be replaced by fully autonomous structures (Kongsberg, 2017).

Global Navigation Satellite Systems (GNSS) for autonomous vessels is a combination of several systems, including GPS, Inertial Motion Units (IMU), and a gyrocompass, used in a system responsible for autonomous navigation. “It is expected that the GNSS receiver will be the primary source of position information for the autonomous ship” (Felski & Zwolak, 2020). “Being such widely used and essential tool GPS is becoming an attractive target for criminals and hackers” (Ahmad et al., 2019). Therefore, this system will be fully responsible for keeping the vessel in position, so resilience to threats for this system is essential. Busnel, in 2016, presented six groups vulnerable to threats resulting from the operation of the GNSS system (**Figure 3**). Cybersecurity threats for GNSS system mainly include spoofing and cyber-attacks.

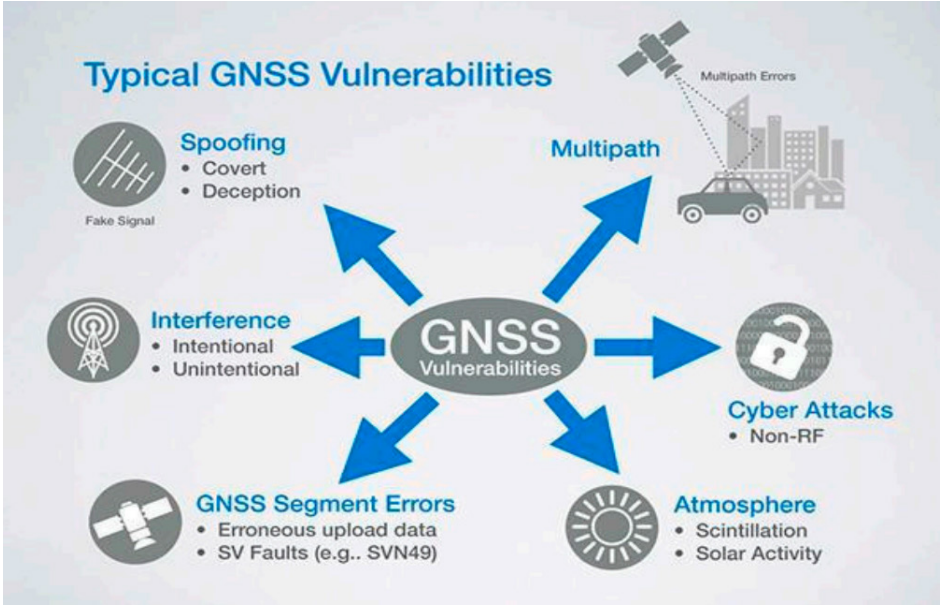

Figure 3 Threats resulting from the GNSS system.
Source: Felski and Zwolak (2020).

"Spoofer is a device that simulates mimic (false or spoof) satellite signals, transmits onto the target receiver to alter the PVT information" (Warner et al., 2012).

3. Current ship safety systems

There are three main safety systems that can be found on conventional vessels:

- Ship Security Alert System (SSAS);
- Automatic Identification System (AIS), and
- Global Maritime Distress and Safety System (GMDSS).

3.1. Ship Security Alert System

The Ship Security Alert System is a ship danger warning system. It serves as an enhancement of the ship's security, primarily in the event of a potential pirate or terrorist attack. It is considered as a practical part resulting from the International Ship and Port Security Code (ISPS Code). The system consists of a printed circuit board in a protective box, as well as two buttons and a transmitting antenna. One of the buttons must be placed on the bridge, and the other in a place chosen by the shipowner. In the event of a potential attack, a button that initiates the transmission of a signal through Inmarsat satellites has to be pressed. Then, the signal is received by coastal stations. In the next step, information about the pirate attack is transferred to the Company Security Officer (CSO) and the company managing the SSAS system. This allows the attacked ship to be located and help sent.

Some Safety Management Manuals (SMMs) contain references to the safety of on-board information systems. However, these references to information security or computer security are usually very basic. For example, an SMM will relate to on-board computer security measures, such as password protection and backups. The main emphasis is on the security of Operational Technology (OT). According to Bermejo, cybersecurity should be more embedded in the SSP and SMM. Cybersecurity procedures should include the following issues (Bermejo, 2010):

- The existence of a contingency plan for ECDIS navigation systems;
- A contingency plan for information technology systems, And
- An internet access security policy setting out the restrictions that apply, depending on the vessel's operations.

3.2 Automatic Identification System

The Automatic Identification System is a system responsible for the automatic identification of ships and data exchange between ships. According to the requirements of Chapter V of the International Convention for the Safety of Life at Sea (SOLAS) developed by the IMO (IMO, 2021c), the AIS system should be fitted on commercial ships with a tonnage above 300 Gross Register Tonnage (GRT), and on all passenger ships, regardless of their tonnage. AIS is an unencrypted transponder that provides ship information such as course, speed, current position, and ship type.

The AIS system improves vessel traffic management and safety. On the other hand, AIS messages are transmitted as plain text, which in turn can be a potential risk, as they can be read by anyone. AIS attacks can affect, in general, the confidentiality, integrity, availability, possession, authenticity, and utility of information. These characteristics are called the Parkerian Hexad (Parker, 2015).

Based on the risk assessment model for Automatic Dependent Surveillance - Broadcast (ADS-B) (Gauthier & Seker, 2018), five categories of threats have been identified that may also apply to the AIS system (Strohmeier, 2015).

- Eavesdropping - this is the simplest possible attack, because AIS is a radio system operating on the VHF frequency, and is also unencrypted;
- Jamming - this can occur at the ground station level or from the ship level and jam radio signals, so that the AIS system will refuse access;
- Message injection - this consists of sending false information about ship traffic communication, due to the fact that the AIS system is unencrypted and the sources of the information sent are not verified;
- Message deletion - this is done by interfering with the sequence of bits of information, making the messages unable to be read on the receiver's side, and
- Message modification - this method consists of changing the value of individual bits into their reciprocal, e.g., from 1 to 0.

3.3 Global Maritime Distress and Safety System

The Global Maritime Distress and Safety System has been designed to obtain assistance as soon as possible in the event of an emergency. This system is composed of several subsystems (Ilcev, 2020; Korcz, 2017; Shishkin & Koshevoy, 2013):

- Inmarsat satellite radiocommunication;
- Satellite alerting and locating objects in danger - COSPAS-SARSAT;
- Radar location using SART transponders;
- DSC - Digital Selective Calling;
- NBDP long band radiotelegraphy;
- SSB radiotelephony;
- VHF radiotelephony, and
- Navigational warnings distribution - NAVTEX.

The cyber risk analysis for Cyber-Enabled Ships (C-ES) in a work (Kavallieratos & Katsikas, 2020) shows that the GMDSS system on vessels is the second system (after ECDIS) exposed to cyber-attacks. Selected threats related to the GMDSS system, along with the requirements that must be met for a cyber-attack to occur, are presented in **Table 1**.

Table 1 Potential threats to the GMDSS system, along with the requirements that must be met for such a threat to occur.

Threat	Requirement
Spoofing	Distress signals transmitted through the GMDSS must be verified by external actors, such as Shore Control Center (SCC) and other ship subsystems, such as the Autonomous Engine Monitoring and Control (AEMC) and Navigation systems
Tampering	The signals transmitted to external actors or subsystems must be appropriately encrypted
Repudiation	The authenticity of the transmitted GMDSS signals and data in transit to the Autonomous Ship Controller (ASC) to other subsystems and to the SCC must be ensured
Information Disclosure	The measures used to protect the confidentiality and integrity of data should not downgrade their utility

Source: Own elaboration, based on Kavallieratos and Katsikas (2020).

4. Current resolutions

4.1 International Safety Management Code

The International Safety Management (ISM) Code was introduced by the IMO and entered into force in May 1994 as an international law (Ghosh & Abeysiriwardhane, 2021; IMO, 2021b). The ISM code applies to all vessels with a capacity above 500 GRT. It enforced the creation of an individual safety management system by shipping companies, often extended to the Quality and Safety Management System (QSMS) (Chruzik, 2020). The most important provisions of the ISM Code relating to ships are:

- The development of a ship maintenance program in terms of the minimum occurrence of failure or accident, and
- Periodic control of all devices that have been assigned critical importance in the system.

From the 1st of January 2021, cybersecurity as a concept has also been implemented in the ISM Code (DNV GL, 2020).

4.2 International Ship and Port Security Code

Following the terrorist attacks on the 11th of September 2001, the International Ship and Port Security Code (ISPS) was established. This code was developed on the 9th - 13th of December 2002 and came into force on the 1st of July 2004. It was attached to the SOLAS convention through chapter XI-2 (Special Measures to Enhance Maritime Security). The regulations concern:

- All passenger ships;
- Cargo ships over 500 GRT;
- Mobile drilling units, and
- Port facilities serving the above mentioned ships on international voyages.

The ISPS code consists of two parts: A and B. The first part details the requirements for ships and ports. Part B, on the other hand, describes the guidelines on how to interpret and apply the rules. The ISPS Code requires ships to be equipped with the following systems and components (Witherbys, 2015):

- An Automated Identification System;
- A legible IMO number on the hull of the ship;
- A Ship Security Plan and a Ship Security Officer, and
- A ship security system.

There are 3 security levels (Wardani, 2021; Ng & Vaggelas, 2012). The actions of a ship's crew must be adapted to each of the levels. Level 1 defines normal conditions and standard procedures that do not require special protection conditions. Level 2 is introduced when there may be an increased risk of terrorism, or when passing through a region threatened by piracy. Level 3 is set when an attack has already occurred in a given region, or when there are indications of a potential threat; for example, when a message about a bomb planted on a ship is received. It is also important that the same level of security must apply to the ship and the port facility. If the security levels are different, the level with the higher security standard becomes the applicable level.

5. Piracy in the 21st century

5.1 Traditional piracy

Despite the implementation of modern technology, traditional piracy is still a reality. According to the annual report published by ICC International Maritime Bureau, the number of piracy and armed robbery incidents that took place in 2020 increased to 195, in comparison to 162 in 2019 (IMB, 2021). The main areas exposed to pirate attacks were the Gulf of Guinea, the Indian Ocean, the Strait of Malacca, and the South China Sea (Zhang et al., 2021; Quốc & Nguyen, 2019; UNCTAD, 2014). Nowadays, pirates use data about ships, such as information about the ship's location from the AIS system. An emphasis in this paper is on digital means; therefore, other details in relation to activities in traditional piracy will not be provided here.

5.2 Cyber piracy

At the same time, another significant problem is to ensure the cybersecurity of ships. Industry 4.0 also reaches maritime transportation. One of the defining concepts of Industry 4.0 is "Industry 4.0 utilizing the power of communications technology and innovative inventions to boost the development of the manufacturing industry" (Kagermann et al., 2013). The maritime Industry 4.0 includes intelligent subsystems that connect various mechanisms on a ship into one network. In the future, the ship as a whole will be completely managed from shore and, hence, all information will be transmitted wirelessly. Here emerges the possibility to manipulate the data transmitted between the ship and the Shore Control Station.

In 2017, I.H.S. Fairplay conducted a maritime cyber security survey, to which 284 people responded. 34 % of them said that their company had experienced a cyber-attack in the previous 12 months (Rider, 2018).

The first major global cyber-attack related to the maritime industry took place in June 2017. The Danish shipping company Maersk fell victim to the NotPetya attack. This was a series of cyber-attacks carried out using software that pretended to be ransomware. This malware attack crashed the Maersk vessel management system. The losses suffered by the company amounted to 300 million USD (Lika et al., 2018; Fayi, 2018).

In the first half of 2020, hacker activity was reported to have increased by 400 % (Security Magazine, 2020). This means that ships could be expected to be attacked more often.

The Wago company, in response to the emerging cyber-attacks, has proposed solutions of the "IT-Security by Design" type, which means that cybersecurity will be implemented in the form of layers in the control structure being built. A ship will be divided into restricted access segments, with division into subnets and monitoring systems at different levels of ship automation. Technical solutions already exist. For example, this can be achieved by building a virtual private network (VPN) based on OpenVPN with SSL / TLS (Secure Sockets Layer, Transport Layer Security) connections. Such connections also allow for encrypted data transmission wirelessly (Südekum & Bannholzer, 2020).

5.3 Types of cyber threats

In version 4 of BIMCO's publication of "The Guidelines on Cybersecurity Onboard Ships", cyber threats are classified into two main groups- untargeted attacks and targeted attacks (BIMCO, 2021).

Untargeted attacks are attacks that use techniques available on the Internet. Examples of such tools and techniques are:

- Malware: A general term for harmful software designed to damage a computer system without the knowledge of the owner. Some of the common types and names for malware include spyware, viruses, worms, and trojans (MITAGS, 2021).
- Water Holing: This consists of creating a fake website, which will collect data entered by unaware users.

Targeted attacks are more sophisticated and use tools specifically designed for targeting a certain company or ship (BIMCO, 2021):

- Social Engineering: Manipulating people in order to extract confidential information.
- Brute Force: Using programs that try to guess the access password.
- Denial of Service: This type consists of flooding the servers with a large amount of information, which makes it impossible for users to gain access to the data.
- Spear-phishing: This type of attack is similar to phishing but is focused on a specific person or company.
- Subverting the Supply Chain: "occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data" (Korolov, 2021).
- Impersonation: This consists of impersonating an employee in order to steal data.
- Phishing: Attacks of this type involve sending large numbers of e-mails to people impersonating someone else in order to steal data or gain access to such data.

6. Navigation systems for autonomous ships most vulnerable to cyber attacks

STRIDE is a model of threats developed by Garg and Kohnfelder at Microsoft for identifying computer security threats. STRIDE is an acronym for six cyber threats for each category (Honkaranta et al., 2021):

- Spoofing;
- Tampering;
- Repudiation;
- Information disclosure;
- Denial of service, and
- Elevation of privilege.

Kavallieratos et al. (2019) saw the authors using the STRIDE method to examine the level of potential cyber threats to autonomous ships. As a result of their research, it was found that the AIS and ECDIS systems are among the most vulnerable navigation systems for autonomous ships.

6.1 AIS

The problem that arises with this device is the unlimited access to certain information about ships, which can violate the privacy of companies and, most importantly, facilitate attack planning by pirates. The threats to this system include ghost ships that are created to force other ships to change their course. It is also possible to send false weather information or generate false information about collisions.

As stated by Tam and Jones (2018), "Unmanned ships may attract more competitors and activists as the likelihood of being caught is considerably lower given the attacker resources are significant enough to obfuscate or hide their activity, e.g. use denial of service (DoS) attack on surveillance".

6.2 GPS

The Global Positioning System (GPS) can be vulnerable to data spoofing. According to Tam and Jones (2018), "Moreover, loss of GNSS can result in the failure of other ship systems (e.g., AIS) as many are highly dependent on satellite position".

In the case of the GPS system, such attacks are based on broadcasting a false GPS signal in such a way that the receiver incorrectly estimates its position. Such an experiment was carried out by students on a luxury yacht (Saarinen, 2013). In a device the size of a suitcase, a transmitter was placed, which initially gave a position consistent with that received by the ship's GPS. The signal received by the yacht from the GPS satellites was gradually replaced by the signal emitted from the GPS spoofing device, thanks to which control over the yacht's navigation system was obtained. This made it possible to change the yacht's course, while on the electronic plotter, the yacht's course did not change.

Another type of the attack is jamming the GPS signal. Devices used for that purpose are able to jam the GPS signal reception within a range of 3 to 400 m.

According to the Safety and Shipping Review 2017, in the period from 2012 to 2017, there were several incidents related to cyber security. One of them was reported as "South Korea reported that hundreds of its vessels had to return to the port, as their GPS signals were jammed due to a cyber-attack initiated by North Korea" (Allianz Global Corporate & Specialty, 2017).

6.3 ECDIS

Nowadays, paper maps have been completely removed from use. In their place, electronic maps, in the form of the Electronic Chart Display and Information System (ECDIS), have emerged. These systems are more than a digital alternative to traditional maps, as such devices collect data from various systems installed on the ship and are able to display it and use it as an aid to the navigation of the ship. The input data include AIS, GPS, log, anemometer, and radar. The system has to be connected to the internet to receive the latest digital map data.

In January 2014, the NCC Group launched a trial hacker attack to gain access to a ship's ICS. According to CyberKeel, several security weaknesses were detected, including the ability to read, download, replace, or delete any file stored on a distribution server of electronic maps (Hayes, 2016). ECDIS can be also infected with malware via a USB port (Heering, 2020). Selected threats related to the ECDIS system are shown in **Table 2**.

Table 2 Potential threats to the ECDIS system, along with the requirements that must be met for such a threat to occur.
Source: Own elaboration, based on Kavallieratos and Katsikas (2020).

Threat	Requirement
Spoofing	The use of ECDIS must be restricted only to authorized and well trained personnel.
Tampering	The ECDIS must be able to control the flow of voyage-related data sent to other ships and to the SCC.
Repudiation	The ECDIS should be able to audit sent and received data to external actors.
Denial of Service	Communication between the ECDIS and the satellite system should be continuously available.

Regular software and hardware updates are crucial (Heering, 2020). In many cases, Windows XP and Windows 7 are still used on workstation PCs for the running of ECDIS software (Dyryavyy, 2014).

7. Conclusions

In connection with the development trends of maritime transport and, thus, with the increased risk of virtual crimes, it should be emphasized that cyber-attacks are an upcoming problem. Currently, the industry and regulations concerning cybersecurity are at an early stage of development; however, early preparation and implementation of solutions against cyber-attacks, and making people aware of the risk, will enable the avoidance of potential threats. Until now, the IMO has issued guidelines on maritime cyber risk management. "The guidelines provide high-level recommendations on maritime cyber risk management" (IMO, 2021a). Additionally, much more extensive guidelines were issued by the BIMCO organization (BIMCO, 2021).

The navigation systems used for autonomous ships that are most vulnerable to cyber-attacks presented in the article show that, already at this level, the security of ships from the virtual side is low, and there will be more and more systems exposed to attacks. Also, the described legal resolutions mainly concern traditional piracy, and cybersecurity is just being introduced.

Early preparation and implementation of solutions aimed at cybersecurity will decrease the likelihood of future attacks and, at the same time, reduce the potential damage caused by cyber-attacks.

References

Ahmad, M., Farid, M. A., Ahmed, S., Saeed, K., Asharf, M., & Akhtar, U. (2019). *Impact and detection of GPS spoofing and countermeasures against spoofing* (pp. 1-8). In Proceedings of the 2nd International Conference on Computing, Mathematics and Engineering Technologies. Sukkur, Pakistan. https://doi.org/10.1109/ICOMET.2019.8673518

Allianz Global Corporate & Speciality. (2017). *Safety and shipping review 2017*. Retrieved from https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review-2017.pdf

Bermejo, A. G. (2010). *Maritime cybersecurity using ISPS and ISM codes*. Retrieved from https://www.he-alert.org/filemanager/root/site_assets/standalone_article_pdfs_1220-/he01335.pdf

BIMCO (Baltic and International Maritime Council). (2021). *The guidelines on cyber security onboard ships*. Retrieved from https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Chruzik, K. (2020). Integration model of management systems in sea transport. *International Journal on Marine Navigation and Safety of Sea Transportation, 14*(2), 393-396. https://doi.org/10.12716/1001.14.02.16

DNV GL. (2020). *Cyber security to be covered in SMS from 1 January 2021: Aare you prepared?* Retrieved from https://www.dnv.com/news/cyber-security-to-be-covered-in-sms-from-1-january-2021-are-you-prepared--176620

Dyryavyy, Y. (2014). *Preparing for cyber battleships: Electronic chart display and information system security.* Retrieved from https://www.nccgroup.com/ae/our-research/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security

Fayi, S. (2018). *What Petya/NotPetya ransomware is and what its remidiations are* (pp. 93-100). Information Technology - New Generations. https://doi.org/10.1007/978-3-319-77028-4_15

Felski, A., & Zwolak, K. (2020). The ocean-going autonomous ship: Challenges and threats. *Journal of Marine Science and Engineering, 8*, 41. https://doi.org/10.3390/jmse8010041

Gauthier, R., & Seker, R. (2018). *Addressing operator privacy in automatic dependent surveillance: Broadcast (ADS-B)* (pp. 52-61). In Proceedings of the 51st Hawaii

International Conference on System Sciences. Waikoloa Village, USA. https://doi.org/10.24251/HICSS.2018.693

Ghosh, S., & Abeysiriwardhane, A. (2021). The influence of information technology on the implementation of the International Safety Management (ISM) Code: A shift from paper-based to paperless ships. *Maritime Technology and Research, 3*(3), 299-311. https://doi.org/10.33175/mtr.2021.249024

Hayes, C. R. (2016). *Maritime cybersecurity: The future of national security*. Calhoun. Retrieved from https://calhoun.nps.edu/handle/10945/49484

Heering, D. (2020). Ensuring cybersecurity in shipping: Reference to Estonian shipowners. *International Journal on Marine Navigation and Safety of Sea Transportation, 14*(2), 271-278. https://doi.org/10.12716/1001.14.02.01

Honkaranta, A., Leppänen T., & Costin, A. (2021). *Towards practical cybersecurity mapping of STRIDE and CWE: A multi-perspective approach* (pp. 150-159). In Proceedings of the 29th Conference of Open Innovations Association. Tampere, Finland. https://doi.org/10.23919/FRUCT52173.2021.9435453

Ilcev, M. (2020). New aspects for modernization global maritime distress and safety system (GMDSS). *International Journal on Marine Navigation and Safety of Sea Transportation, 14*(4), 991-998. https://doi.org/10.12716/1001.14.04.26

IMB (2021). *ICC-IMB piracy and armed robbery against ships report-01 January-31 December 2020*. Retrieved from https://www.icc-ccs.org/reports/2020_Annual_Piracy_Report.pdf

IMO (International Maritime Organization). (2021a). *Maritime cyber risk*. Retrieved from https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

IMO (International Maritime Organization). (2021b). *The International Safety Management (ISM) Code*. Retrieved from https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx

IMO (International Maritime Organization). (2021c). *International Convention for the Safety of Life at Sea (SOLAS)*. Retrieved from https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

Jović, M., Tijan, E., Marx, R., & Gebhard, B. (2019). Big data management in maritime transport, Pomorski zbornik. *Journal of Maritime and Transportation Science, 57*, 123-141.

Kagermann, H., Wahlster, W., & Johannes, H. (2013). *Recommendations for implementing the strategic initiative industrie 4.0*. acatech - National Academy of Science and Engineering.

Kavallieratos, G., & Katsikas, S. (2020). Managing cyber security risks of the cyber-enabled ship. *Journal of Marine Science and Engineering, 8*(10), 768. https://doi.org/10.3390/jmse8100768

Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2019). Cyber-attacks against the autonomous ship. *Lecture Notes in Computer Science, 11387*, 20-36. https://doi.org/10.1007/978-3-030-12786-2_2

Kongsberg Maritime. (2015). *K-IMS enhance efficiency and safety*. Retrieved from https://www.kongsberg.com/globalassets/maritime/km-products/documents/k-ims.pdf

Kongsberg. (2017). *Autonomous ship project, key facts about Yara Birkeland*. Retrieved from https://www.kongsberg.com/maritime/support/themes/autonomous-ship-project-key-facts-about-yara-birkeland

Korcz, K. (2017). Some aspects of the modernization plan for the GMDSS. *International Journal on Marine Navigation and Safety of Sea Transportation, 11*(1), 167-174. https://doi.org/10.12716/1001.11.01.20

Korolov, M. (2021). *Supply chain attacks show why you should be wary of third-party providers*. Retrieved from https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html

Lika, R. A., Murugiah, D., Brohi, S. N., & Ramasamy, D. (2018). NotPetya: Cyber attack prevention through awareness via gamification (pp. 1-6). In Proceedings of the 2018

International Conference on Smart Computing and Electronic Enterprise. Shah Alam, Malaysia. https://doi.org/10.1109/ICSCEE.2018.8538431

Line, M. B., Nordland, O., Røstad, L., & Tøndel, I. A. (2006). *Safety vs. Security?* In Proceedings of the 8th International Conference on Probabilistic Safety Assessment & Management. ASME Press. https://doi.org/10.1115/1.802442.paper151

Lloyd's Register, QinetiQ and University of Southampton. (2015). *Global marine technology trends 2030.* Retrieved from https://www.lr.org/en/insights/global-marine-trends-2030/global-marine-technology-trends-2030

Mingyu, K., Tae-Hwan, J., Byongug, J., & Han-Seon, P. (2020). Autonomous shipping and its impact on regulations, technologies, and industries. *Journal of International Maritime Safety, Environmental Affairs, and Shipping, 4*(2), 17-25. https://doi.org/10.1080/25725084.2020.1779427

MITGAS. (2021). *Guide to ship cybersecurity*. Retrieved form https://www.mitags.org/guide-ship-cybersecurity

MUNIN. (2015). *Maritime unmanned navigation through intelligence in networks*. Retrieved from http://www.unmanned-ship.org/munin/about

Ng, A. K. Y. & Vaggelas, G. K. (2012). *Port security: The ISPS code* (pp. 674-700). In Talley, W. K. (Eds.). *The Blackwell companion to Maritime Economics*. Wiley-Blackwell. https://doi.org/10.1002/9781444345667.ch33

Özköse, H., Ari, E. S., & Gencer, C. (2015). Yesterday, today and tomorrow of big data. *Procedia - Social and Behavioral Sciences, 195*, 1042-1050. https://doi.org/10.1016/j.sbspro.2015.06.147

Parker, D. B. (2015). Toward a new framework for information security? In Bosworth, S., Kabay, M. E., & Whyne, E. (Eds.). Computer security handbook. 6th ed. John Wiley & Sons.

Quốc-Tiến, L., & Nguyen, C. (2019). Impact of piracy on maritime transport and technical solutions for prevention. *International Journal of Civil Engineering and Technology, 10*, 958-969.

Raunek, K. (2016). *Technologies to make an ultimate eco-friendly ship*. Retrieved from https://www.marineinsight.com/infographics-2/infographics-make-ultimate-eco-friendly-ship

Rider, D. (2018). *Cyber security at sea: The real threats*. Retrieved from https://www.maritime-executive.com/blog/cyber-security-at-sea-the-real-threats

Saarinen, J. (2013). *Students hijack luxury yacht with GPS spoofing*. Retrieved from https://www.itnews.com.au/news/students-hijack-luxury-yacht-with-gps-spoofing-351659

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6), 165-176.

Security Magazine. (2020). *Maritime industry sees 400% increase in attempted cyberattacks since February 2020.* Retrieved from https://www.securitymagazine.com/articles/92541-maritime-industry-sees-400-increase-in-attempted-cyberattacks-since-february-2020

Shishkin, A. V., & Koshevoy, V.M. (2013). Stealthy information transmission in the terrestrial gmdss radiotelephone communication. *International Journal on Marine Navigation and Safety of Sea Transportation, 7*(4), 541-548. https://doi.org/10.12716/1001.07.04.09

Sivan, A. P., Johns, J., & Venugopal, J. (2014). Big data intelligence in logistics based on hadoop and map reduce. *International Journal of Innovative Research in Science, Engineering and Technology, 3*(3), 2634-2640.

Strohmeier, M., Lenders, V., & Martinovic, I. (2015). On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Communications Surveys & Tutorials, 17*(2), 1066-1087. https://doi.org/10.1109/COMST.2014.2365951

Südekum, N., & Bannholzer, E. (2020). *Cybersecurity on ships*. Retrieved from https://www.wago.com/gb/marine-offshore-solution/cybersecurity-on-ships

Tam, K., & Jones, K. (2018). *Cyber-risk assessment for autonomous ships* (pp. 1-8). In Proceedings of the 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). https://doi.org/10.1109/CyberSecPODS.2018.8560690

Trelleborg Marine Systems. (2018). *Use of big data in the maritime industry*. Retrieved from https://www.patersonsimons.com/wp-content/uploads/2018/06/TMS_SmartPort_InsightBee_Report-to-GUIDE_01.02.18.pdf

UNCTAD. (2014). *Maritime piracy. Part I - An overview of trends, costs and trade-related implications.* Retrieved from https://unctad.org/system/files/official-document/dtltlb2013d1_en.pdf

UNCTAD. (2020). *Review of maritime transport 2020.* Retrieved from https://unctad.org/topic/transport-and-trade-logistics/review-of-maritime-transport

UNODC. (2013). *Comprehensive study on cybercrime.* Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Wardani, A. (2021). Maritime security arrangements relating to standard security of ships and port facility based international ship and port facility security code 2002 and implementation in Indonesia. *Lampung Journal of International Law, 3*(1), 19-28. https://doi.org/10.25041/lajil.v3i1.1985

Warner, J. S., Johnston, R., & Cpp Los Alamos. (2012). A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *The Journal of Security Administration, 25*(10), 19-28.

Witherbys. (2015). *21st Century seamanship*. Witherby Publishing Group.

Xingan, L. (2008). *Cybercrime and deterrence: Networking legal systems*. The Networked Information.

Yoo, Y., & Park, H. S. (2021). Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. *Journal of Marine Science and Engineering, 9*(6), 565. https://doi.org/10.3390/jmse9060565

Zhang, L., Guo, L., Zhang , X., & Zhang, P. (2021). Legal issues on wage protection of seafarers held hostage by pirates. *Maritime Technology and Research, 3*(3), 268-279. https://doi.org/10.33175/mtr.2021.248808