MBNA Publishing House Constanta 2022

Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

Aspects of cyber security in the field of maritime transport

To cite this article: R. Moinescu, C. Răcuciu, D. Glăvan, S. Eftimie, Proceedings of the International Scientific Conference SEA-CONF 2022, pg. 124-134.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-22-016

Aspects of cyber security in the field of maritime transport

Radu MOINESCU, Ciprian RĂCUCIU, Dragoș GLĂVAN, Sergiu EFTIMIE

Military Technical Academy "*Ferdinand I*"
radu.moinescu@gmail.com

Abstract. The global shipping industry is increasingly connected to and dependent on Communication and Information Systems. Failure to prepare, plan and deal with cyber-attacks can have very unfortunate consequences for companies that will be subject to such attacks. This paper examines the factors that can lead to cyber-attacks targeting the shipping industry.

1. State of affairs

Throughout its field of activity, the global shipping industry is increasingly connected and dependent on information systems. Failure to prepare, plan and address cyber threats can have unpleasant consequences for companies that will be the target of cyber-attacks.

Information and communications technology infrastructure supports services and goods such as energy, transportation, telecommunications, financial services, etc., which are essential for a nation's prosperity. Given their importance, it is necessary to protect these vital information infrastructures in strengthening the prosperity of a society. Therefore, this issue is an area of concern for international policy makers.

The target audience of this paper is organizations, national authorities, government agencies and private companies involved in the maritime sector and in particular in cybersecurity.

Specifically, the research covers policy makers and other relevant stakeholders (e.g., port authorities) involved in the development and implementation of security policies and good practices for the maritime

2. Cybersecurity in the field of maritime transport

2.1 Maritime transport as an economic sector

The shipping sector is vital to the global economy. According to a statistical survey conducted in a Eurostat study for Europe in 2021, about 52% of freight traffic was at sea, up from just 45% a decade ago. [1] This growing dependence on maritime transport underlines its vital importance for European society and the economy. As can be seen in other economic sectors, maritime activity is increasingly relying on information and communication technology to optimize its activities. Information and communication technology is being used more and more to enable basic maritime operations, from navigation to propulsion, from cargo handling to traffic control communications etc.

According to data published by the National Institute of Statistics in Romania, in 2021 53.121 million tons of goods were loaded / unloaded. Compared to 2020, there was an increase of 15.6% in loaded goods and 9.4% in unloaded goods. [2]

The ability of Romanian shipowners to make immediate decisions for the sale and purchase of ships and, to a large extent, the successful identification of the right points for entry or exit in investments are credited with this performance.

2.2 Threats and security in cyberspace

Over the last decade, as cyber threats have increased, they have spread to all sectors of the industry that are gradually relying on information and communication systems. Recent examples of deliberately disrupting critical automation systems, such as Stuxnet, demonstrate that cyberattacks can have a significant impact on critical infrastructure. The disruption or unavailability of such information and communication systems could have catastrophic consequences for the governments of the European Member States and for social welfare in general. The need to ensure the reliability and robustness of information and communication systems against cyber-attacks is a key challenge at national and pan-European level.

This first analysis of cyber security issues in the maritime sector identified key perspectives and ideas in this area. It also addresses the policy framework at European level and places the issue of cyber security in the maritime sector as the next logical step in the global effort to protect information infrastructure. This document identifies key areas of concern as well as ongoing initiatives that could serve as a basis for the development of cybersecurity in this particular context. Finally, high-level recommendations are presented for each observation, indicating possible approaches that could be taken to address these risks.

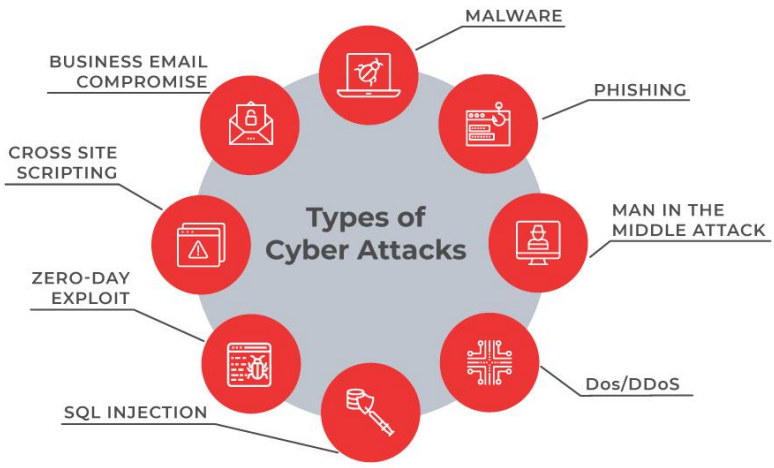

Fig. 1. Types of Cyber Attacks [3]

Shipping companies and the operation of the shipping industry are based on information systems. Positioning systems (GPS / GLONASS), electronic certificates, tracking / monitoring of goods, electronic navigation (ECDIS), automatic identification systems (AIS), communications and record keeping are some of the activities that depend on the reliability and security of information systems. This dependence on computer systems and computer networks, especially those connected to the Internet, creates opportunities for cyber-attacks as a result of poor security practices.

The driving forces of cyberspace are *time*, *space*, *anonymity*, *asymmetry* and *efficiency*. These factors create the concept of "TSAAE" which influences the reality and understanding of security. [4]

If a person or organization does not understand these key factors of the TSAAE, there will be an increased likelihood of failure and loss of strategic advantage. The concept emphasizes a new approach to understanding security. Because cyberspace is a flexible environment, these driving forces manifest differently in the physical world.

Time is a vital and irreplaceable part of human life. Every action, preparation and implementation take time. In the natural world, physical threats generally do not occur immediately. For example, it takes time to mobilize troops or forces to fight. In cyberspace, however, actions can be seen in no time

and without warning, or for a longer period of time. In terms of time, it doesn't matter if a cyber-attack starts from the house next door or from the other side of the world.

Space is intertwined with time at a complex level. In cyberspace, no one is immune to a cyber-attack, and anyone can launch a cyber-attack on the digital battlefield. In the worst case, a cyber-attack only requires an individual to press the "enter" key. In cyberspace, any target can be attacked immediately. Cyberspace has not been stable and is constantly changing with technology updates and network changes. In the long run, cyberspace may change in the direction of international conventions and directives. The challenge in cyberspace is the difficulty of determining the impact of a cyber-attack and where it started.

The main challenge to anonymity is to identify cyberspace and its functions. Identification refers to the identity of entities and the indication of their position, which is difficult in cyberspace. The level of certainty of identification depends on three factors: the level of targeting of the identification, the nature of the actions and the objective of the identification pursued. Sometimes politically motivated groups claim responsibility for a cyber-attack. For example, the US government has been unofficially involved in the creation and implementation of Stuxnet malware, which affected Iran's nuclear program in 2011. This has shown the world that some countries have both the power and the resources to use cyber weapons. advanced on request.

The term asymmetry is quite old, but it became part of the public debate after the September 11, 2001 attacks in which Al Qaeda waged an asymmetric war. Asymmetric warfare exploits the weakness of an opponent and tries to exploit the competitive advantage in the best possible way. Cyberspace creates new opportunities for asymmetric warfare. Every operational function based on cyberspace, including information warfare, is asymmetric in nature. Asymmetry characterizes cyber threats. It also contains limited possibilities for identifying cyber-threatening agents and offers the possibility to use these tools through non-state actors, which are specific to individuals or organizations that have significant political influence but do not belong to a particular country. Asymmetry allows cyber-attacks to take advantage of changes faster and easier.

The effectiveness of a cyber-attack does not mean making Internet connections unavailable. The purpose of the cyber-attack is usually to undermine the credibility and way in which organizations and nations operate without interruption. The key element of cyber efficiency is that the operator can perform several actions simultaneously in different sizes. The larger the operating network used by organizations and nations, the more networks and information systems need to be protected. In terms of effectiveness, non-state actors have two ways of exerting strategic influence. First, they can leverage their own cyber security capabilities and collaborate with state actors or other non-governmental organizations. Second, they can form various alliances, for example with national authorities providing cybersecurity capabilities. Although cyberspace can be used for malicious activities, it has created a platform for new functions / features such as digitization, virtualization and automation. Thanks to these innovations, organizations have been able to hire various intermediaries through their production and service chains.

2.3 Risks

The five most common and basic five cyber risks are:

- human actions and (non-compliant) behavior, as well as lack of technical knowledge;
- the interdependencies that appear in the business chain;
- mixed use of private and professional transactions in the use of mobile devices;
- vulnerable computer systems that are not completely up to date;
- software for which secure programming has not been performed.

Threat factors can be classified into one of seven categories: [5]

- individuals, for example, 'script kiddies' and insiders;
- activist groups, also known as "hacktivists";
- commercial competitors;
- cyber criminals;
- terrorists;

- nation states and state sponsored actors.

Any of these threat factors are equally relevant to: elements of remote ship operating systems, delivery information / data stored on external servers; services provided by third parties and the ship's supply chain. When analyzing the potential threats posed by the hostile entities listed above, it is important to recognize that there may be some convergence between the goals and objectives of individual groups. For example, certain malware, developed by cybercrime groups, includes sophisticated manipulation and control functions, allowing information to be securely deleted and modular components to be updated to deliver new or varied farms over time. Thus, a machine or device that was initially compromised for financial crimes could be used in the future to access sensitive data or to provide a backdoor to allow attacks on ships themselves.

3. Cyber-attack situations

3.1 Attacks on navigation systems

Security breaches and cyber-attacks on the bridge's navigation systems have been reported. ECDIS, AIS and GPS are essential aids to navigation and have all been found to be vulnerable to cyber-attack.

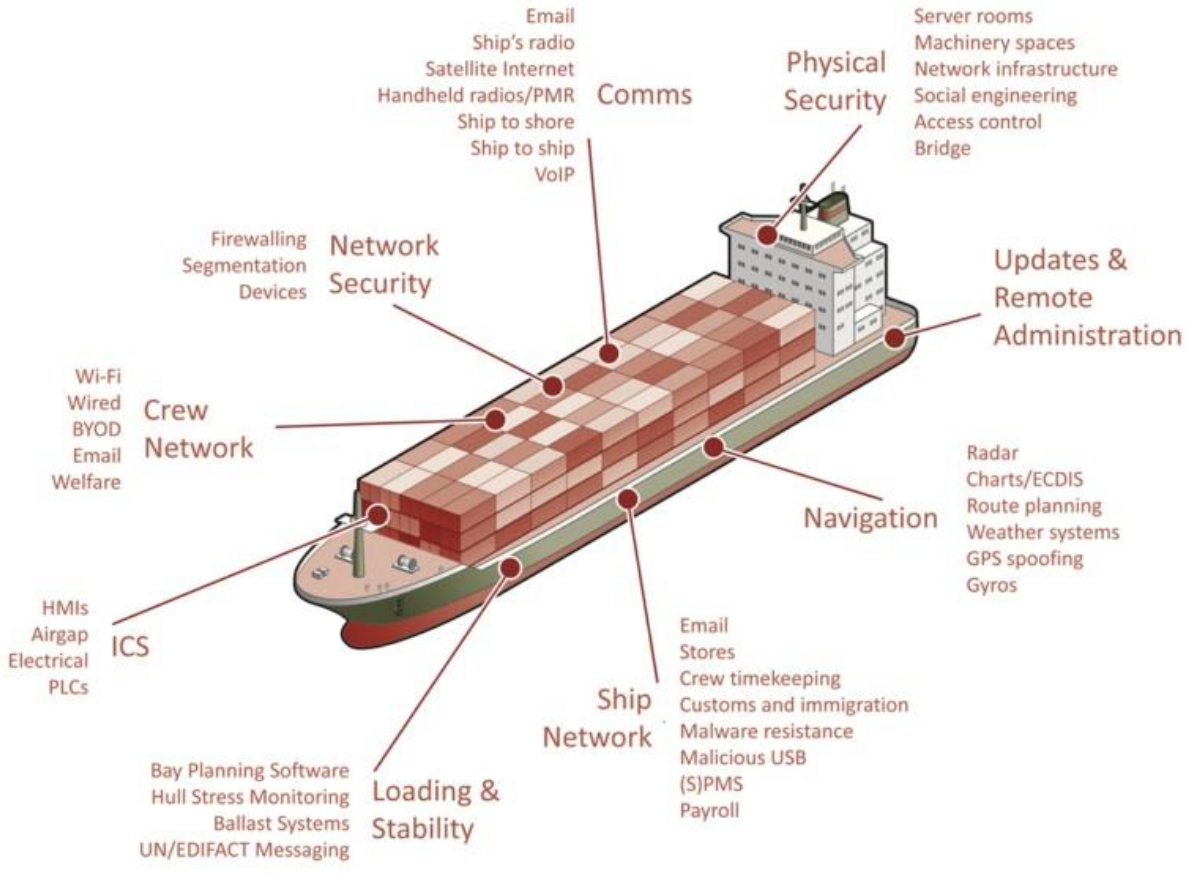

Fig. 3. What does a ship look like to an attacker? [20]

The International Maritime Organization (IMO) is the United Nations agency for the safety of navigation. This organization imposed the mandatory installation of AIS for all passenger and merchant ships over 500GT and ships over 300GT engaged in international trade. This capability has been in place since 2004. [6] IMO regulations require AIS to be able to automatically exchange information on identity, type, location, route, speed, navigation status and other relevant safety information with other

ships, ground installations and aircraft. AIS has been used as a navigation tool for ships as an alternative to radar and is an important tool for controlling ships when passing through VTS (Vessel Traffic Services).

Because AIS does not have its own encryption system, it makes it a vulnerable target for cyber-attacks, as demonstrated by a study by cybersecurity company TrendMicro. The study found and experimentally demonstrated that AIS could prevent the ship from providing accurate information about its movements, cargo, etc. and created a ghost ship with a false GPS position, and dangerous cargo, causing other AIS users to see this wrong warning signal. [7]

On July 23, 2013, a team of researchers at the University of Texas at Austin, USA, managed to deflect a $ 80 million yacht from its course using a stronger localized signal that provided false information to the ship's GPS receivers. The attack was in the form of a consultation exercise with the shipowner, without informing the crew, except for the captain. With equipment totaling $ 3,000, the researchers were able to confuse the GPS antennas, sending their own positions, and thus gain full control of navigation. The result was that they were able to change the course of the yacht without the crew noticing, as the navigation systems did not deviate from the planned route. [8] Like AIS and GPS for civilian use, it is neither encrypted nor authenticated and is therefore an easy target. With 90% of global passenger and freight transport being based on GPS technology, we need to better understand the implications of spoofing the signal of this sensor time.

It can be argued that the relatively low public profile of most shipping companies indicates that they are less likely to be cyber-attacked than financial institutions, energy companies, utilities or gas companies. This can happen; however, the threat is real and the results of a successful attack could be devastating. Of course, the lack of code embedded in the important systems used on board for navigation means that shipping can be considered a "soft" target for an attack and this perception is sufficient to initiate an attack.

The MIT Technology Review stated that the devices needed to intercept and transmit false AIS and GPS signals cost about 700 Euros, which makes it possible for an individual with the necessary technical skills to use them for malicious purposes. [9]

Of course, some shipping companies have a high degree of visibility. An attack on the cyber perimeter of a cruise ship, which would disrupt its navigation system, would have received high media attention from the event, and in serious cases could have been a loss of life. and would have caused significant damage to assets.

The IMO has recognized since 2004 that the publication of AIS data on the Internet and elsewhere would jeopardize the safety and security of ships and port facilities. The IMO subsequently condemned those who made the data public and encouraged national governments to discourage its publication. However, the MIT Technology Review reported that when Trend Micro expressed concern about the IMO following its flagship attack on AIS in 2013, the IMO responded that it could only respond to a government-submitted paper. IMO member or an advisory organization. When asked in June 2014, the IMO confirmed that the cyber threat was not being debated by any member and was therefore not on its work schedule at the time. [10]

In any case, it would take some time to update the existing protocol and regulations to deal with the current threat, and it would take much longer to replace equipment in the global fleet with new, more secure systems. At the same time, the potential threat remains and is undoubtedly growing.

The realistic answer to a threat is to consider the likelihood of an event occurring that could cause a loss that could occur in relation to both the expected and maximum negative results if the event occurred. Once the likelihood and potential consequences are understood, informed decisions can be made about risk mitigation and transfer. However, this conventional approach to risk management is not applicable to the cyber threat, due to a specific exclusion from insurance policies.

3.2 Damage to information integrity

In late 2013, Belgian authorities revealed that the container terminal in Antwerp was the target of a cyber-attack by smugglers. The attack on the port of Antwerp is believed to have taken place over a

two-year period in June 2011. The attackers gained access to the terminal's operating systems, ordering the release of containers into their own trucks and thus circumventing official customs controls. Once the command was executed, the data was deleted by the intruders without leaving any traces. This led to the handling of smuggled cargo. Police in a relevant investigation following the identification of the attack found a large number of drugs, weapons and large sums of money in a container. It is not known how many containers the attackers managed to smuggle into. The organized crime group hid cocaine in containers in South America containing bananas and lumber. The attackers accessed the port's computer systems through a security breach, identified the exact location of the containers of interest in the port, and then changed their location and delivery times. The organized crime group then sent its own drivers to pick up the containers before the scheduled pick-up. [11][12]

Port authorities were first alerted to the incident when entire containers began to disappear from the port without explanation. The compromise of the computer systems in the port took place in a series of stages, starting with the sending of malware to the employees of at least two companies operating in the port of Antwerp. [11][12]

3.3 Damage caused by malware

The most eloquent example is the attack on A.P. Moller-Maersk since June 2017. The attack, which caused significant operational difficulties on several ships, as well as the closure of 76 terminals, affecting the handling of thousands of containers was caused by NotPetya malware. The malware was distributed through a Ukrainian accounting software called MeDoc, used for filing tax returns in Ukraine. The MeDoc software contained backdoors in the software users' networks, which were used by malware to enter through the software's automatic update system. Although the recovery of the operation and the elimination of the risk were very fast, according to the company, the consequences of the attack caused damages of 300 million euros. It all came down to the opening of an email with a malicious attachment received by a Ukrainian company employee. [13]

The attack was successfully carried out regardless of the measures that Maersk took for such events. In its 2016 annual report, the agency clearly stated the following: “A.P. Moller-Maersk is involved in complex and large-scale global services and is committed to increasing the digitalization of its business, making it highly dependent on IT operating systems. "Risk is addressed through close monitoring and improved cyber resilience and an emphasis on business continuity management when IT systems are affected, despite their efforts." [14]

Although the incident was serious, the organization responded quickly, under the supervision of the CEO and the management team. A team of IT experts (including internal and external partners) was mobilized to identify, detect and remove malware from affected systems to restore functionality, while at the same time managing mass-media communication was excellent with immediate feedback to stakeholders on the situation in Maersk.

Specifically, the following actions were taken: [15]

- Søren Skou, CEO of Maersk, participated in all requests and crisis meetings to provide immediate guidance;
- internal and external communications were established: Maersk sent daily updates indicating which ports were open and closed, which reservation systems were in operation and much more;
- a customer-focused response has been established. The company's front-line staff is trained to take all necessary measures to satisfy customers, regardless of cost.

Eight days after the attack, Maersk was able to continue making reservations online, although some terminals (e.g., India) had to be managed manually.

Following the cyber-attack, Maersk appears to have taken a new approach to cyber security. To further enhance cyber resilience, numerous immediate and long-term initiatives have been implemented and planned to secure digital business, strengthen information infrastructure, enhance the continuity and recovery of IT and communications services, and strengthen follow-up plans. of the activity. Cyber security equipment and services have been purchased to mitigate some of the potential negative financial

impact of successful cyber-attacks in the future. While in its annual report before the attack, the word "cyber" appeared several times, in its annual report at the end of 2017, "cyber" was found 39 times in the document in addition, cyber risk was included in the relevant matrix as an important factor to be evaluated. [16]

4. Strategies against cyber-attacks targeting the maritime transport sector

4.1 Statistics on cyber attacks

An important focus of the problem we are discussing in this paper is the damage caused by cyber-attacks. The malicious act is the direct cause of the loss, although the consequences may include property damage, personal injury, financial loss or other damages.

The year 2021 saw the highest average cost of a breach of data loss in the last 17 years, rising from $ 3.86 million to $ 4.24 million, a price on an annual basis. The most common cause of data breach was compromising the user's login information. Being a commonly used type of attack vector, it was responsible for 20% of breaches, with security breaches costing an average of $ 4.37 million. [17]

36% of the breaches were related to phishing attacks, an increase of 11%, which could be partly attributed to the COVID-19 pandemic. As expected, the adaptation and adjustment of phishing campaigns by malicious actors was even more visible, depending on the news of the moment. Social engineering attacks are the most serious threats to the public administration, accounting for 69% of all attacks analyzed by Verizon in 2021 targeting institutions in this sector. [18] Not only the frequency of attacks has increased, but also the cost of managing and mitigating violations.

Directive (EU) 2016/1148 on the security of networks and information systems and Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, introduce mandatory notifications of contracts and fines for violating these rules. They can further raise the board's awareness of cyber risks and, as a result, boost cybersecurity requirements for European companies.

From 2021, the IMO will make it mandatory to manage cyber operational risk on board ships. The Committee on Safe Seas (MSC) adopted in June 2017 Resolution MSC.428 (98) on cyber risk management in the maritime security management system. The resolution stipulates that it is necessary to implement an accredited security system for cyber risk management, in accordance with the objectives and requirements of the ISM Code. The directives set out the following actions that can be taken to support the effective management of cyberspace: [19]

- identification of systems, data, which, if attacked, pose a risk to the ship's operations;
- implementation of risk control processes and measures, as well as an emergency plan to protect against a cyber event and to ensure the continuity of transport operations;
- developing and implementing the defense procedures and tools needed to detect a cyber-attack in a timely manner;
- developing and implementing activities and plans to ensure resilience and to restore systems needed for shipping operations or services affected by a cyber event;
- identification of the backup and restoration measures of the computer systems necessary for the maritime transport operations affected by a cyber event.

Resolution MSC.428 (98) encourages IMO Member States to ensure that cyber threats are addressed by existing security management systems (as defined in the ISM Code) no later than the first annual inspection of the company's compliance document after 1 January 2021.

4.2 The need for a strategy against cyber attacks

The emergence of a new social threat in the form of cyber-attacks creates an urgent need for adequate risk mitigation and transfer mechanisms.

Cyber-attacks on ship's operating systems may intentionally or unintentionally affect the operation of the systems and therefore affect the safety of navigation and the safety of ships in general. It is

therefore important for shipowners to include the threat of cyber-attacks in individual ship risk assessments.

Public reports of cyber-attacks on ship operating systems are generally limited. There are probably several explanations for this. One could be that cyber segmentation and security in general is so strong that cyber-attacks on operating systems are difficult to achieve. Another explanation could be that the typical actors of cyber threats, which usually target administrative systems, are simply not interested in these operating systems.

However, behind the low number of reported incidents, there are likely to be significant unreported incidents, as shipping companies are either reluctant to report and talk about the incident in public or because the attacks went unnoticed. Many shipping companies do not monitor or scan their operating systems, which increases the likelihood of unidentified malware.

Part of the threat comes from cybercriminals who threaten computer and communications systems to exploit computing power, storage or communication to make money. Such compromised systems can be used, for example, by cybercriminals to generate cryptocurrencies through so-called mining or as platforms for additional / subsequent attacks. There is also the threat of cyber-attacks that use ransomware as an attack vector, but there is currently no specific interest in ship operating systems. Rather, it is used to attack computer and communications systems belonging to sectors that are vulnerable to their attack techniques. Ship operating systems can be attractive targets for cybercriminals, as they are vital to the shipping company, which can serve as a lever against the victim to pay the ransom. In addition, some types of ransomwares have been programmed to spread autonomously across connected systems and networks. This has been the case since the 2017 WannaCry attacks, when more than 300,000 computers worldwide were infected with ransomware.

4.3 Security of maritime information and communication systems

The security of the on-board IT and communications system depends on the effectiveness of the company's security policy, based on the outcome of the risk assessment. Control of entry points and physical control of the network on a ship may be limited because cyber risk management has not been taken into account in the construction of the ship. It is recommended to design the network structure and how to control it for all new ships.

It is necessary to avoid direct communication between an uncontrolled and a controlled network. In addition, various protection measures need to be added:

- application of network segmentation and / or traffic management;
- managing encryption protocols to ensure the right level of confidentiality and commercial communication;
- managing the use of certificates to verify the origin of digitally signed documents, software or services.

In general, only equipment or systems that need to communicate with each other over the network will be required to do so. The basic principle must be that the interconnection of equipment or systems is determined by operational needs.

4.4 Physical structure of the information and communication system

The physical layout of the network must be carefully examined. It is important to consider the physical location of key network devices, including servers, switches, firewalls, and connections. This will help restrict access and maintain the physical security of the network installation and control of the network access points.

Any design of the IT network will need to include the infrastructure for network management and administration. This may include installing network management software on workstations and dedicated servers that offer file sharing, email, and other network services.

4.5 Network segmentation

Segmentation is the process of dividing a network into smaller areas. In carrying out the segmentation process, it is important to know the logical distribution of the resources necessary to ensure the proper functioning of the organization.

Integrated networks should normally include:

- the necessary communication between the equipment of the operational technology;
- configuration and monitoring of operational technology equipment;
- administrative and production activities, including e-mail and file sharing;
- recreational internet access for crew and / or passengers / guests.

Effective segmentation of the computer network is a key aspect of in-depth defense. Computer equipment, operational technology, and public networks should be separated or segmented by appropriate safeguards. The safeguards used may include, but are not limited to, an appropriate combination of the following:

- perimeter firewall between the on-board computer network and the Internet;
- switches between each network segment;
- internal firewalls between each network segment;
- virtual local area networks / data diodes to host separate segments.

In addition, each segment should have its own range of IP addresses. Network segmentation does not eliminate the need for systems in each segment to be configured with appropriate network access controls and anti-malware software and firewalls.

Segmentation reduces the propagation area of an attack and prevents lateral movement within the network. Segmentation needs to be applied to more areas of the ship. By segmenting, the flow of traffic between subnets becomes easier to control, but you can allow or deny traffic based on a variety of factors, or you can go as far as blocking the entire flow of traffic if necessary. Also, by segmenting, the performance of the network can be increased by closing the traffic only in certain parts of the network that need to see it and can help to locate the technical problems in the network more easily. In addition, network segmentation can prevent unauthorized network traffic, or an ongoing attack from reaching critical parts of the network, and simplify network traffic monitoring work.

5. Conclusions

The information and communication systems used by shipping companies to meet the requirements of the 20th century are now practically proven and cannot respond to the threats of the 21st century. The vulnerabilities that exist in these sensitive systems are an open door and it is only a matter of time before malicious entities that plan to attack them do so.

On-board operating systems are particularly vulnerable if they are connected directly to the Internet without proper security measures or if they have not been adequately protected against malware by external drives. In recent years, the shipping industry has largely focused on the risk of malware infections through open USB ports in operating system hardware.

It should also be noted at the end of the paper that operating system providers have increased access to the network of ships to monitor and update the systems. This can allow cyber-attacks through trusted equipment vendors. Some of the specialist ship equipment suppliers have very large market shares worldwide. A cyber-attack by such a provider could affect the operation and security of a large number of ships throughout the transport industry.

Cyber-attacks can damage operating systems and therefore threaten the security of navigation and the security of ships in general.

Ships' operating systems are usually separated from administrative networks connected to the Internet and are therefore better protected against cyber-attacks. However, the isolation and segmentation of these operating systems is accessible to more and more terrestrial administrative systems. In addition, equipment suppliers have more frequent access to system monitoring and updating. systems update.

This development has provided many business benefits to shipping companies and equipment suppliers, but also allows cyber-attacks by threat agents, which can exploit the vulnerabilities created by digitization and Internet connection. Ships' operating systems are particularly vulnerable if new systems or segmentation changes are installed with little emphasis on cyber security. Cyber-attacks on ship's operating systems may intentionally or unintentionally affect the operation of the systems and therefore affect the safety of navigation and the overall safety of ships. It is therefore important for shipping companies to include the threat of cyber-attacks in risk assessments of individual ships. Unreported incidents call into question the evaluation process.

Any business can be vulnerable to cyber-attacks, and the issue requires a holistic approach to addressing it, which should include:

- raising awareness about cyber-attacks, conducting training and communication on risks at all levels of the company;
- aligning cyber risks with existing security and safety risk management requirements contained in ISPS and ISM codes;
- inclusion of requirements related to the formation, operation and maintenance of critical cyber systems;
- the use of firewalls, anti-malware software, data diodes and encryption devices in computer and communications systems;
- the existence of adequate protection at all levels of the company as part of the safety culture on land and on board.

Public reports of cyber-attacks on ship operating systems are generally limited. There are probably several explanations for this. It could be argued that cyber security is generally so stable that cyber-attacks on operating systems are difficult to achieve. Another explanation could be that typical threat agents, which usually target administrative systems, are simply not interested in these operating systems.

However, behind the low number of reported incidents, there are likely to be significant unreported incidents because shipping companies are either reluctant to report and speak publicly about incidents or because the attacks went unnoticed.

References:

[1] Eurostat, *International trade in goods by mode of transport*, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=International_trade_in_goods_by_mode_of_transport&stable=0, accessed on March 23, 2022

[2] Institutul Național de Statistică, *Transportul portuar de mărfuri și pasageri în anul 2021*, https://insse.ro/cms/sites/default/files/field/publicatii/transportul_portuar_de_marfuri_si_pasageri_anul_2021.pdf, accessed on March 23, 2022

[3] Team Ecosystm, *Things you need to know about Cyber Attacks, Threats & Risks*, March 05, 2019, https://blog.ecosystm360.com/cyber-attacks-threats-risks/, accessed on March 23, 2022

[4] CIO&Leader, *The Changing Reality of Security*, December 12, 2013, https://www.cioandleader.com/articles/10059/the-changing-reality-of-security, accessed on March 23, 2022

[5] The Institution of Engineering and Technology, *Code of Practice: Cyber Security for Ships*, United Kingdom, ISBN 978-1-78561-577-1, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf, accessed on March 23, 2022

[6] International Maritime Organization, *Resolution A.1106(29) - Revised Guidelines for The Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)*, https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/AIS/Resolution%20A.1106(29).pdf, accessed on March 23, 2022

[7] Marco BALDUZZI, Kyle WILHOIT, Alessandro PASTA, *A Security Evaluation of AIS*, Trend Micro, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-

papers/wp-a-security-evaluation-of-ais.pdf, accessed on March 23, 2022
[8] The University of Texas at Austin, *UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea*, July 29, 2013, https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/, accessed on March 23, 2022
[9] Tom SIMONITE, *Ship Tracking Hack Makes Tankers Vanish from View*, MIT Technology Review, October 18, 2013, https://www.technologyreview.com/2013/10/18/82918/ship-tracking-hack-makes-tankers-vanish-from-view/, accessed on March 23, 2022
[10] Marsh, *The Risk of Cyber-attack to the Maritime Sector*, Marsh, July, 2014, https://csdsafrica.org/wp-content/uploads/2017/10/The-Risk-of-Cyber-Attack-to-the-Maritime-Sector-07-2014-1.pdf, accessed on March 23, 2022
[11] Europol, *Hackers deployed to facilitate drug smuggling*, June 2013, https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf, accessed on March 23, 2022
[12] Steve BELL, *Cyber-attacks and underground activities in Port of Antwerp*, BullGuard, October 21, 2013, https://www.bullguard.com/blog/2013/10/cyber-attacks-and-underground-activities-in-port-of-antwerp.html, accessed on March 23, 2022
[13] Michael MIMOSO, *Maersk Shipping Reports $300M Loss Stemming from NotPetya Attack*, ThreatPost, August 16, 2017, https://threatpost.com/maersk-shipping-reports-300m-loss-stemming-from-notpetya-attack/127477/, accessed on March 23, 2022
[14] A.P. Moller-Maersk, *Annual Report 2016*, https://investor.maersk.com/static-files/a31c7bbc-577a-49df-9214-aef2d649a9f5, accessed on March 23, 2022
[15] Richard MILNE, *Maersk CEO Soren Skou on surviving a cyber-attack*, Financial Times, August 13, 2017, https://www.ft.com/content/785711bc-7c1b-11e7-9108-edda0bcbc928, accessed on March 23, 2022
[16] A.P. Moller-Maersk, *Annual Report 2017*, https://investor.maersk.com/static-files/250c3398-7850-4c00-8afe-4dbd874e2a85, accessed on March 23, 2022
[17] IBM, *Cost of a Data Breach Report 2021*, IBM, July, 2021, https://www.ibm.com/security/data-breach, accessed on March 23, 2022
[18] Verizon, *Data Breach Investigations Report 2021*, https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf, accessed on March 23, 2022
[19] International Maritime Organization, *Maritime cyber risk*, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx, accessed on March 23, 2022
[20] PenTestPartners, *Maritime cyber security*, https://www.pentestpartners.com/penetration-testing-services/maritime-cyber-security-testing/, accessed on March 23, 2022