Information & Security

B. Mednikarov, Y. Tsonev & A. Lazarov
vol. 47, no. 1 (2020): 27-43
https://doi.org/10.11610/isij.4702

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Analysis of Cybersecurity Issues in the Maritime Industry

Boyan Mednikarov , ***Yuliyan Tsonev*** , ***Andon Lazarov*** (✉)

Nikola Vaptsarov Naval Academy, Varna, Bulgaria, http://naval-acad.bg/en

ABSTRACT:

The maritime industry with its main components—port logistics, ships, cargo and container distribution systems, autonomous control and navigation systems, global identification and navigation systems—is a substantial and plausible target of cyberattacks. The goal of the present study is to reveal and describe all components of the shipping industry's cybersecurity policy, the main types of cyberattacks, methods, means, and stages of implementation, cyber vulnerability assessment of on-board information and communication systems, as well as technological measures for cyber defence.

ARTICLE INFO:

RECEIVED: 28 Jun 2020
REVISED: 31 AUG 2020
ONLINE: 21 SEP 2020

KEYWORDS:

cybersecurity, cyberattack, maritime industry, ship's computer networks, ship's cyber defence

1. Introduction

The maritime industry with its computerized organizations, companies, ships, ports, storages, navigation, and communication systems on-board, ashore, and in the space is under risk of cybercriminal penetration. The maritime cyber incident can arise in each data pattern of communication exchange.

The cybersecurity problems of the shipping industry attract the attention of many authors in the maritime field. The future trend in the maritime industry indicates that all the logistics resources relate to each other and form integrated autonomous operating systems based on IT-platforms, next-generation smart

✉ E-mail: a.lazarov@naval-acad.bg

shipping rapidly embraces advanced technologies such as machine learning and artificial intelligence.[1] The vulnerabilities to cyber-attacks of today's marine transportation system are problems of substantial importance. The little-known challenges of maritime cybersecurity and vulnerabilities of shipboard systems, oil rigs, cargo, and port operations are subject of significant practical and research interest.[2, 3, 4]

A detailed analysis of the ship's cybersecurity problems in the systems and components installed on mariner ships and systems placed ashore vulnerable to cyber-attacks is provided in [5]. Security metrics serve as a powerful tool for shipping companies to evaluate the effectiveness of protecting computer networks. One approach is via a stochastic security framework to obtain quantitative measures of security by considering the dynamic attributes associated with vulnerabilities that can change over time.[6] The security and safety of the ships at the sea are achieved by using different maritime mechanisms and systems functioning together and simultaneously. The systems are used to monitoring and tracking mariner vessels to ensuring immediate support and help in case of distress. These systems ensure the shipping industry to be on the right track and the position to react adequately and properly during the period of ship exploitation. Anish Wankhede analyses eight maritime systems that ensure ship safety and security and provides important data for the overall smooth running of the shipping industry.[7]

A cyber-attack is any type of offensive criminal action that targets computer information systems, infrastructures, computer networks, or personal computer devices, using various methods to steal, alter, or destroy data or information systems. Melnick presents an analysis of ten common types of cyber-attacks.[8] A number of international organisations provide a thorough description of the ship's cyber-security components and guidelines to ensure the detection of vulnerability and cyber-defence measures taken on-board.[9]

Maritime cybersecurity is a problem which despite getting increasing attention, is still a major reason for concerns. The scale of the issues their cost and potential impacts on the reputation and ability of the maritime industry to operate properly in this environment are highlighted in the high-professional report.[10] The activity of intruders who exploit the zero-day vulnerabilities and prediction of their attack timing is subject of significant interest.[11] Based on the prediction, a method of security measurement is developed to compute optimal attack timing from the perspective of an attacker, using a long-term game to estimate the risk of being found and then choose the optimal timing based on the risk and profit.

The contemporary cyberattacks are carried out with new and diverse malware. There exist a variety of methods to detect, analyse, and defend against these attacks. The malware detected by these methods includes advanced present threat attacks, which allow additional intervention by attackers. Such malware presents a variety of threats (DNS, C&C - DNS tunnel for communication with the C&C server, Malicious IP, etc.).

A decision-making methodology to identify threat sources and malicious activities based on the analysis of various types of malware that occur during collection processes and machine learning based on a quantitative analysis of these threat sources and activities are proposed in [12].

An analysis of various vulnerability patterns their causes and consequences, the vulnerabilities of IBS components using various cyber-attack techniques e.g., jamming, spoofing, and hijacking, is provided in the review,[13] where the baseline for future investigation of Integrated Bridge System (IBS) vulnerabilities and maritime cybersecurity is outlined. Ship computer networks generate a significant volume of behavioural system logs and data traffic. The severity associated with vulnerabilities and the ever-changing vector of cybercriminals' attacks is in the focus of Shahzad and co-authors.[14]

An exceptional solution, able to provide a high detection rate with an acceptable false alarm rate and anomaly-based Intrusion Detection System as a key factor in network security due to its ability to cope with unknown attacks and new security threats is defined by Callegari, Giordano, and Pagano.[15] In contemporary electronic navigation, the mandatory use of official paper nautical charts is replaced using Electronic Chart Display and Information Systems (ECDIS). It operates with Electronic Navigational Charts (ENCs) – geospatial databases of the Geographic Information System (GIS) for real-time navigation. ENCs are compiled according to the strict IHO technical specifications.[16]

The criminal cyber impact is expressed in violation of the normal functioning of the software and computer systems for data processing and ship's systems management. Responsible for the ship's cybersecurity are its command, personnel, management, and coastal service personnel. This includes assessing and managing the risk of cyber impacts on confidential information, especially that directly related to ship security, active and passive protection of electronic and computer systems.

The goal of the present work is to generalize and systemize the components of the maritime industry from the position of the cybersecurity and cyber defence, to suggest a tactical and technical interpretation of criminal cyber intrusion, detection, and prevention, to outline main cyber threats, measures to protect, requirements to computer networks, main navigation, communication and managing components on the mariner vessels and ashore equipment.

2. Cyberattacks: Methods, Means, and Stages of Implementation

2.1. Types of Cyberattacks in the Shipping Industry

Cyberattacks are both targeted and untargeted. Targeted attacks are cyber-attacks on specific corporate Internet networks and network components with a specific purpose of penetration - access to confidential information, obstruction of the normal functioning of ship systems. Untargeted attacks are carried out using Internet environment and software tools to detect unprotected communication components.

Types of Untargeted Attacks

To the most popular untargeted cyber-attacks can be referred: [5, 8]

Malware – aimed to access or damage a computer from the network of the ship or shipping company, it includes Trojans, spyware, ransomware, viruses, and worms.

Ransomware – this is a cyberattack with software that encrypts data files on individual workstations or databases, which the user does not have access to until the ransom is paid.

Phishing – this is an attack with emails to multiple user addresses to access personal and/or confidential information, request to visit a fake web site, and other fraudulent activities.

Types of Targeted Attacks

Targeted attacks are carried out with software tools and techniques specifically designed to affect ships and shipping companies. Tools and techniques for targeted attacks include: [5, 8, 9]

Social engineering - this is a non-technical approach to cyber-attacks, used to manipulate and force personnel to violate security requirements, usually, but not exclusively, through interaction through social media.

Brute force – this is a cyber-attack through repeated attempts to decipher the password of the network or network device.

Denial of service (*DoS*) – this is a classic cyber-attack to prevent authorized users from accessing information, usually by flooding network devices (computers and servers) with data.

Man-in-the middle – a form of active eavesdropping attack in which the attacker intercepts to read or modify data communications to masquerade as one or more of the ship's entities involved.

Supply chain – an adversary inserts vulnerability in hardware or software of the ship or shipping company to manipulate those systems at the developer, assembly, or designer's location. Can be activated at a later point in time without direct access by the attacker.

Spoofing – a false signal is broadcasted with the intent to mislead the victim receiver, such as a Global Positioning System or email user.

3. Stages of Cyberattack in the Maritime Industry

The following stages of targeted cyberattacks can be identified: [9]

- *Intelligence (investigation/reconnaissance)* - the first stage of preparation for a cyberattack.
- *System Access (Delivery)* - the second step, intruders access the system data of maritime companies.
- *Penetration (violation)* – the third step determined by the vulnerability of the system and the method of penetration into the system.
- *Pivot penetration* – the fourth step, penetration into the control system of the machines and units of the ship.

4. Vulnerability Assessment of On-board Information and Communication Systems from Cyberattacks

The ship's administration is assessing potential cyber threats and assessing the cyber resilience of on-board systems, through experts in the maritime industry who are developing a strategy to assess cyber risk response.[8]

Cargo management systems – Cargo management systems include digital systems used for loading, managing, and controlling the movement of goods, including dangerous goods, on-board communication systems for interaction with shore-based logistics centres, including port facilities and sea terminals (Fig. 1).

Figure 1: Cosco shipping port from Shanghai International Port Group.[21] Source: https://www.seatrade-maritime.com/asia/cosco-shipping-port-sells-port-assets-sipg https://www.seatrade-maritime.com/sites/seatrade-maritime.com/files/styles/article_featured_retina/public/uploads/2019/09/SIPG.jpg

Modern seaports operate with complex logistics, transport networks, and management systems (Fig. 2). The port management systems, equipped with navigation and communication systems to track the maritime cargo from the source point to the destination, are subject to cyber-attacks that can cause significant technical problems and financial losses.[19, 20] For example, the cybercriminals can infiltrate by remote terminal into the port's computer network manipulate cargo documentation, and release smuggled cargo.

The penetration of the systems can allow the criminals to control whether their shipping containers are regarded as suspicious by the police or customs authorities.

Integrated Bridge systems - the modern bridge command system is a computer-based ship cyber-physical system the functionality of which is provided

Figure 2: Los Angeles port. Source: https://limacharlienews.com/business/americas-failed-seaports.[20]

by local Internet network technologies, satellite communication, and navigation systems making the bridge system vulnerable to cyberattacks.[13]

ECDIS is compliant with International Maritime Organization.[16, 19] A main component of ECDIS is the Geographic Information System (Fig. 3). The computer-based communication and navigation management system ECDIS would allow a cybercriminal to access, read, download, replace or delete any file stored on the machine hosting ECDIS as well as to modify or delete contents of files and charts on shipboard or onshore computers.[19, 22] Once such unauthorized access is gained, attackers could be able to interact with the workstation or servers of shipboard and shore networks.

The attack could be made through USB key ports or file downloading from the Internet.[2] In 2014 agents from NCC Group investigate ECDIS's cyber protection. After penetrating the system by physical USB port and Internet, the agents can download, read, modify, replace and delete files stored on the ECDIS computer, to use the computer network on shipboard and interact with all network devices

Automatic Identification System (AIS) enables ships to communicate with other ships, exchange positional data, and avoid collisions with other ships, reefs, floating objects, etc. (Fig. 4). AIS is one of the most vulnerable ship's systems.[2, 5] An attacker with a VHF radio could exploit AIS weaknesses and intercept transmitted by AIS data (e.g., vessels' identity, type, position, heading, and speed to shore stations).[9, 17] The attacker could also compromise and tamper with the data, impersonate port authorities, communicate with the ship or effectively shut down communications between ships and between ships and ports, send false weather forecast information to a vessel to enforce to divert

Figure 3: ECDIS.
Source: https://www.seanews.com.tr/most-vessels-subject-to-solas-now-ready-for-electronic-chart-display/161511/.

the course due to a non-existent storm, impersonate as marine authorities to trick the vessel crew into disabling their AIS transmitter, rendering them invisible to anyone but the attackers themselves, enforce vessels to increase the frequency with which they transmit AIS data, resulting in all vessels and marine authorities to be flooded by data, carrying out, in essence, a denial-of-service attack, fake "closest point of approach" alert can trigger a collision warning alert.[22]

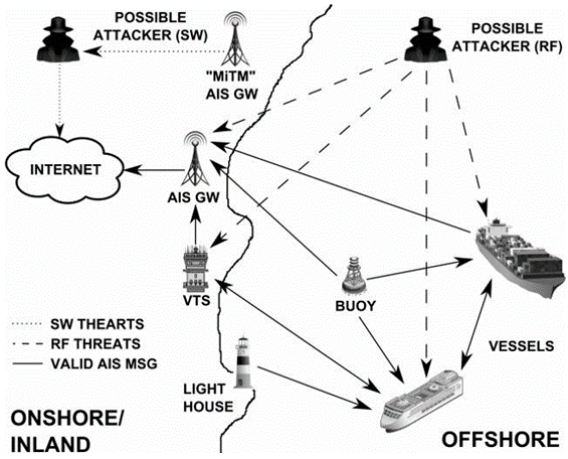

Figure 4: AIS cyberattack. Source: https://doi.org/10.1145/2664243.2664257.[22]

Possible cyber-attacks to AIS are the modification of all ship data regarding position, course, cargo, speed, ship's name, creation of "ghost" vessels at any arbitrary location in the ocean, which would be recognized by AIS receivers as genuine vessels, triggering a false collision warning alert, resulting in a coarse adjustment.[2] In Fig. 5 a possible collision after a fake Closest Point of Approach (CPA) is illustrated.

Figure 5: Possible collision after a fake CPA alert.
Source: https://www.helpnetsecurity.com/

Each maritime vessel is assigned a range of frequencies where it can communicate and exchange information with port authorities, as well as other vessels. There is a specific set of instructions that only port authorities can issue that make the vessel's automatic information system transponder work on a specific frequency. A malicious cybercriminal can spoof this type of "command" and practically switch the target's working frequency to another one which will be blank. This will enforce the vessel to stop transmitting and receiving messages on the right frequency, effectively making it "disappear" and unable it to communicate.

Propulsion and machinery management and power control systems – mechanical and electrical systems of a ship allowing the crew to maintain their basic professional functions throughout exploitation.[3, 7] Some of the systems might be accessible from the shore side like engine performance or Emergency Shut Down Systems (ESD).

Access control systems – these are systems for controlling access to ship's equipment and infrastructure, ensuring the reliability, physical security, and safety of the ship and its cargo, as well as systems for monitoring, announcing, and warning of circumstances related to on-board security.

Passenger servicing and management systems - these are electronic systems for passenger service and management – digital systems used for passenger property management, boarding, and access control; these systems may con-

tain data related to passengers. Also, smart devices, such as tablets, smartphones, scanners, etc.) should be under control, such as potential targets of a cyber-attack.

Passenger network access – the local and Internet network access of passengers is a potential risk to the ship's cybersecurity. Network passenger services, such as Internet access, mail servers, must be outside the on-board computer networks used to control the ship and crew operations.

Administrative and crew welfare systems – onboard computer networks used for administrative management and crew actions are also extremely vulnerable to cyberattacks, especially if they also provide access to the Internet and an email server. This can be used for unauthorized access to onboard systems and data. Therefore, these systems should be considered uncontrolled and should not be linked to a critical safety system on-board. Software provided by ship management companies or owners is also included in this category.

Communication systems – shipboard communication systems for the Internet and satellite and/or other wireless communication increase the risk of cyber-attacks on the ship's systems. This requires the use of reliable software security tools to achieve the necessary cybersecurity.

5. Main Steps of the Ship's Cyber Risk Assessment Process

A cybersecurity risk assessment determines the information-communication systems that could be influenced and by cyberattacks and then identifies the risks affecting those systems and can be performed by the following steps.[9, 23]

Step 1: Preliminary Risk Assessment

Description of the ship's main functions and systems and the corresponding levels of potential cyber impacts. Study of the technical descriptions of IT equipment and operational technological equipment, assessment of the cyber risk of network architectures and structural components, their interfaces, and interaction between the individual devices.

Step 2: Ship Cybersecurity Assessment

The focus of the ship cybersecurity assessment is the information, network, operational and technological equipment, and its documentation, as well as the level of training and education of the ship's crew on measures and actions to ensure cybersecurity. Social engineering is a hacker instrument to enforce, ship's employees to disclose confidential information. Except Spear Fishing, Reverse Social Engineering, the Friendly Hacker is a new instrument to access ship's employees' emails and social media accounts to track their messages, to read and download information of interest. It discloses an opportunity a malicious software to be included. To avoid their privacy intrusion, the ship's employees should not disclose their identity, names, and roles in the ship's company on social networks.

Measuring maritime companies' and ship members' susceptibility to cyberattacks is an approach to quantify, evaluate, and improve the cybersecurity. For example, modelling phishing attacks using a variety of decoy emails against

crew members, educates them to be cautious about suspicious emails.[25] The process includes multiple testing, teaching, and learning. In case the crew member receives a spear-phishing email the event must be reported to be taken appropriate action to protect other crew members. The results of modelling and measuring ship member susceptibility to cyber-attacks can be used as metrics to evaluate and quantitatively determine the meaning of the human factor in the maritime industry's cyber-defence.

Step 3: Review, Assessment, and Report on the Potential Impact of Ship Cyber Vulnerability

Based on the assessment of the ship's cyber vulnerability, an analysis of its potential impact on the operation and functionality of all ship systems is provided. The risk assessment includes summary information on the ship's cybersecurity profile as a whole. Instructions and recommendations are developed on the technical characteristics of devices and systems with a high risk of cyber impact, their operation, and control, assessment of their cyber vulnerability, a priority list of actions to prevent potential impacts on cybersecurity, ship, and elimination the consequences of cyberattacks.

6. Technical and Technological Measures for Cyber Defence

The most effective approach to prevent cyber-attacks and the spread of malware is the mutual separation of the networks according to their purpose and functionality. Networks on ship's boards are segregated trough software firewalls and port configuration of ACLs.

An important part of the ship's network is the network of crew computers, servers, main router, satellite or 4G internet connection, the network for passengers. The Figure presents an example of such a network. The network architecture is divided into four subnetworks.[19] The subnetworks are presented in different colours. Orange coloured are so-called "Business" inner network done only through cables that connect administrative computers and servers. Pink coloured is a link to the ECDIS machine, therefore as well to the rest of the equipment and sensors of the ship. In this case, ECDIS can exchange information between two different networks, namely, regular LAN network and WAN - NMEA 2000. Thus, ECDIS is very vulnerable and the intruder would likely try to attack it to get access to other devices.

As can be seen in Fig. 6, the pink line connection allows accessing the satellite internet directly through Inmarsat Crew Port. The blue line connection has Internet access either through satellite (Inmarsat) or through the regular land GSM/4G access points as long as the ship is within range. Green links denote Wi-Fi networks dedicated for crew's private devices. From the security point of view, it is recommended to apply encryption techniques to the Wi-Fi services.

Consider communication between electronic devices and sensors like an anemometer, gyrocompass, GPS receiver, sonar, autopilot on ship's board usage of basic serial NMEA0183 or NMEA2000 messages protocol. Communications with this protocol do not require authentication, validation nor encryption. Everything goes as plain text. The network test indicates that usually in the ship's

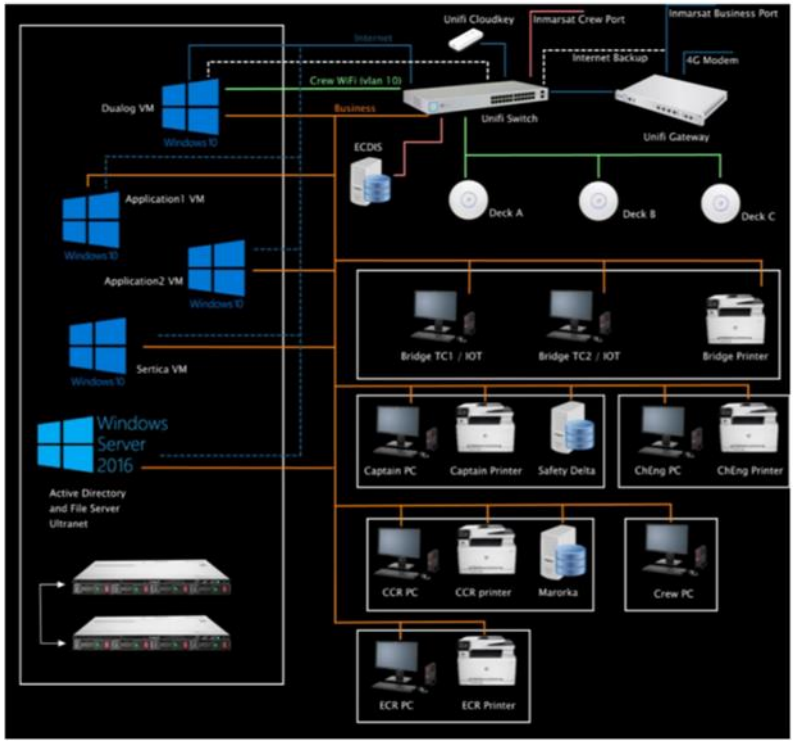

Figure 6: Ship's computer network.
Source: https://doi.org/10.1145/2664243.2664257.

WAN/LAN networks are often bridged together in several points. Based on Figure one main gateway is under the form of ECDIS machine. In this case, a simple attackman in the middle by compromising messages which flows through the network is enough to disturb the normal functionality of devices without notifying anybody or being aware of what happens. Examples of such messages are presented by the following codes.[18]

Code 1:

```
ÝþR15$HEHDT,62.8,T*13
ÝþR11!AIVDV,46,16,0,A,1234567890XX1234567890XXX1234567890,82,232100.06,08,12,2013*4A
ÝþR12$GPZDA,232100.01,08,12,2013,0,0*6E
ÝþR11!AIVDV,47,16,0,A,1234567890XX1234567890XXX1234567890,83,232100.06,08,12,2013*4A
ÝþR16$BNALR,,000,A,V,C1=OFF;C2=12;C3=00*5A
ÝþR11!AIVDV,48,16,0,A,1234567890XX1234567890XXX1234567890,86,232100.10,08,12,2013*47
ÝþR14$GPGLL,1522.5150,N,2806.4014,E,232100.01,A,A*52
```

Code 2:

```
$GPAPA,A,A,0.10,R,N,V,V,011,M,DEST,011,M*82
```

The first code presents captured messages flowing through the ship's sensor part network. All data is visible.

The second code presents the message used by autopilot. The red box around letter R tells the direction of the rudder, in this case, the right direction. Another red box around "82" is just XOR checksum. Edition of these two parameters allows changing movement direction of the ship.

The most effective approach to prevent cyber-attacks and the spread of malware is the mutual separation of networks in dependence of their purpose and functionality. Networks on ship's boards are segregated trough software firewalls and port configuration of ACLs.

6.1. Means Ensuring Physical Cybersecurity

Physical cybersecurity is realized by technical means, which prevent the physical access to critical devices and equipment of the network infrastructure with an emphasis on the ports for access to the network and data, cables, cabinets with communication equipment. For example, ECDIS is a centralized system where information from many sources is concentrated. Penetrating in this system gives access to all management ship information. Physical USB ports of ECDIS are used to update voyage information. With not protected operating system USB ports can be infected with viruses causing ECDIS to display the ship's position in a different place compared to the real position. The problem multiplies in case ECDIS wrong data are sending to AIS system, which resends information in respect of the ship's position and identification to other ships. The fake data cause the neighbour ships' anti-collision system alarm to turn on. Based on the faked anti-collision alarm, captains of neighbour ships are trying to get through a place with virtual high intensity of other ships.

Detection, blocking, and intrusion signals are key features of the Intrusion Detecting System (IDS). Detection of intrusion into network devices with malware, the establishment of the threshold of cyber incidents, means of signaling, warning, and counteraction are the main functions of the network administrators of the ship. For this purpose, a penetration detection system and a system for the prevention of external interference in the network are used as the main functions of the firewall.

6.2. Assessment of Cyber Risk in Space-based and Radio Navigation and Communication

There exists a special type of attack called Meaconing in which the cyber intruder tracks and records the electromagnetic emission from satellites' transmitters and re-transmits it as a stronger signal with a delay to the targeted ship. The ship receiver reads a dominating fake signal. Recently agents from UT Austin demonstrate a spoofing attack on the yacht "White Rose of Drax" sailing on the Mediterranean.[2] A fake powerful signal suppressing the authentic GPS signal is emitted until full control over the ship's navigation system is achieved. To prevent or reduce the risk of this cyberattack the ships must be equipped with GPS, GLONASS, DGPS, and Galileo satellite receivers. It is recommended to use

on-board and onshore anti-jamming and anti-spoofing systems, ships must be equipped with nanosatellite navigation tools.

The ship's space-based, radio-communication, and navigation systems are extremely vulnerable to cyber impacts. This places special demands on on-board communication and navigation systems and access to them. They must be completely disconnected and disconnected from the Internet network infrastructure, which is the responsibility of the ship's administration, and control over its proper functioning is carried out by the ship's network administrator. Action should be provided to limit as far as possible the access of shore-based service stations via radio communication channels to the ship's control systems.

Under special control are the Internet access point, the data traffic from which it must be protected with firewalls, Access Control Lists, and other software and configuration solutions.

To cope with cyber problems with wireless network access control, a certain level of protection, access to wireless networks and components must be secure. A strong encryption key is used, which must be changed regularly.

6.3. Configuration of Hardware Network Components and Software Installation and Setup

The configuration of the hardware and software systems is essential, which should be performed by authorized experts with administrator rights, such as network administrators or crew members with an administrator profile provided. They are also responsible for managing, activating, and deactivating user profiles of crew members. User profiles restrict access to a separate workstation or server and do not allow the user to change the configuration of the network and individual devices, install new programs and applications. It is recommended to use specialized protective software that senses the dynamics of changes in the computer networks as CimTrak, a powerful cybersecurity tool.[26] This software has properties and capabilities to identify: what kind of authorized or unauthorized user makes changes in the network, what kind of changes are made, where the changes happen, when the changes take place, how the changes are realized.

6.4. Email and Web Browser Protection

The communication between the ship and the coast services is done via e-mail, which sets high requirements for the level of protection of the web browser, e-mail addresses, data, and information that is exchanged. between the ship and the shore services. This ensures the protection of shore and on-board personnel from potential 'social engineering', prevents attempts to use the e-mail application to obtain confidential information, ensures the secure exchange of confidential information through encrypted protection, thus achieving confidentiality and integrity of data, preventing web browsers and email clients from executing malicious code. File encryption, deactivation of hyperlinks in the e-mail system, avoiding the use of well-known e-mail addresses, and ensuring that the e-mail system is configured user accounts are used to securely transfer emails.

6.5. Protection of the Ship's Application and System Software

Application and system software installed on computers in the maritime industry affects all areas of computing, communications, and systems' controlling. Its security is of substantial importance to the cyber defence of information and communication systems of ships and the shipping industry. It includes central controlling all critical system software, testing and certificating new and modified software, making backups of all application and system software and databases on-board and ashore. Updating and correcting the application and system software of onboard computer-based systems is a major step in ensuring cybersecurity. Software patches that provide the security of operational technological equipment are included in the periodic maintenance cycle of software systems. These updates or patches are applied so that they cannot be used for cyber impact.

7. Conclusions

The present work can be considered as concise guidelines to meet requirements to the maritime industry in respect of cybersecurity and cyber defence of basic components of vessels and shipping companies. An enlarge list of cyber threats has been provided with an accent on those related with the shipping industry. The main stages of cyberattacks and vulnerabilities of ship systems have been discussed. A special place in this work takes a description of communication and navigation systems on-board and ashore, most vulnerable to cyberattacks part of the ship infrastructure. Special attention has been paid to computer networks and requirements to ensure the cyber defence of the information flow and data traffic for maintenance of the main ship's systems functionality.

References

1 Harri Pyykköa, Jarkko Kuusijärvib, Bilhanan Silverajanc, and Ville Hinkkaa, "The Cyber Threat Preparedness in the Maritime Logistics Industry," *Proceedings of 8th Transport Research Arena*, April 27-30, 2020, Helsinki, Finland, https://www.corealis.eu/wp-content/uploads/2020/05/TRA2020_Cybersecurity_article_Pyykko_et_al.pdf.

2 Joseph DiRenzo, Dana A. Goward, and Fred S. Roberts, "The little-known challenge of maritime cyber security," *6th International Conference on Information, Intelligence, Systems and Applications* (IISA), 6-8 July 2015, https://doi.org/10.1109/IISA.2015.7388071.

3 "Cybersecurity in the Shipping Industry," *Capital Link Cyprus Shipping Forum, Deloitte*, 2019, https://globalmaritimehub.com/wp-content/uploads/attach_852.pdf.

4 Kala Baskar and Mahesh Balakrishnan, "Cyber Preparedness in Maritime Industry," *International Journal of Scientific and Technical Advancements* 5, no 2 (2019): 19-28.

5 Bartlomiej Hyra, "Analyzing the Attack Surface of Ships," DTU Compute Department of Applied Mathematics and Computer Science Technical University of Denmark, Kongens Lyngby, (2019). Available on https://backend.orbit.dtu.dk/ws/portalfiles/portal/174011206/190401_Analyzing_the_Attack_Surface_of_Ships.pdf, accessed 5 May 2020.

[6] Subil Abraham and Suku Nair, "A Predictive Framework for Cybersecurity Analytics Using Attack Graphs," *International Journal of Computer Networks & Communications* 7, no. 1 (2015), https://doi.org/10.5121/IJCNC.2015.7101.

[7] "8 Maritime Systems That Ensures Ship Safety and Security," *Marin Insigh*t, March 20, 2020, https://www.marineinsight.com/marine-safety/8-maritime-systems-that-ensures-ship-safety-and-security/, accessed 14 May 2020.

[8] Jeff Melnick, "Top 10 Most Common Types of Cyber Attacks," *Netwrix Blog*, https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Birthday attack, accessed 14 May 2020.

[9] "The guidelines on cybersecurity onboard ships," version 3, produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, and WORLD SHIPPING COUNCIL, 2018, https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.

[10] "How Big a Problem is Maritime Cyber Security," *Videotel*, February 4, 2019, https://videotel.com/how-big-a-problem-is-maritime-cyber-security/, accessed 12 June 2020.

[11] Lihua Yin, Yanwei Sun, Zhen Wang, Yunchuan Guo, Fenghua Li, and BinxingFang, "Security Measurement for Unknown Threats Based on Attack Preferences," *Hindawi Security and Communication Networks*, 2018, Article ID 7412627, https://doi.org/10.1155/2018/7412627.

[12] Dohoon Kim, "Decision-Making Method for Estimating Malware Risk Index," *Applied Sciences* 9, no. 22 (2019): 4943, https://doi.org/10.3390/app9224943.

[13] Malik Shahzad, Kaleem Awan, and Mohammed A. Al Ghamdi, "Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS)," *Journal of Marine Science and Engineering* 7, no. 10 (2019): 350, doi:10.3390/jmse7100350.

[14] Malik Shahzad, Kaleem Awan, Pete Burnap, and Omer Rana, "Identifying Cyber Risk Hotspots: A Framework for Measuring Temporal Variance in Computer Network Risk," *Elsevier*, *Computers & Security* 57 (2016): 31-46, https://doi.org/10.1016/j.cose.2015.11.003.

[15] Christian Callegari, Stefano Giordano, and Michele Pagano, "An information-theoretic method for the detection of anomalies in network traffic," *Elsevier*, *Computers & Security* 70 (2017): 351-365, https://doi.org/10.1016/j.cose.2017.07.004.

[16] Athanasios Palikaris, and Athanasios K. Mavraeidopoulos, "Electronic Navigational Charts: International Standards and Map Projections," *Journal of Marine Science and Engineering* 8 (2020): 248, https://doi.org/10.3390/jmse8040248.

[17] Marco Balduzzi, Kyle Wilhoit, and Alessandro Pasta, "A Security Evaluation of AIS," *TrendMicro*, https://www.n0secure.org/wp-content/uploads/2016/06/wp-a-security-evaluation-of-ais.pdf.

[18] Ken Munro, "Hacking, Tracking, Stealing and Sinking Ships," *Pen Test Partners, Blog: Maritime Cyber Security, January 4, 2018*, https://www.pentestpartners.com/security-blog/hacking-tracking-stealing-and-sinking-ships/, accessed 20 May 2020.

[19] Katherine Si, "Cosco Shipping Port sells port assets to SIPG," Seatrade Maritime, Sept. 20, 2019, https://www.seatrade-maritime.com/asia/cosco-shipping-port-sells-port-assets-sipg.

[20] Gary Busch, "America's failed seaports – Trump's 'America First' policy isn't the only barrier to free trade," *Lima Charlie News*, 2020, https://limacharlienews.com/ business/americas-failed-seaports/.

[21] Boris Svilicic, David Brčić, Srdjan Žułkin, and David Kalebic, "Raising Awareness on Cyber Security of ECDIS," *Transnav, the International Journal on Marine Navigation and Safety of Sea Transportation* 13, no. 1 (March 2019): 231-236, https://doi.org/10.12716/1001.13.01.24.

[22] Marco Balduzzi, Alessandro Pasta, Kyle Wilhoit, "A security evaluation of AIS automated identification system," *ACSAC '14: Proceedings of the 30th Annual Computer Security Applications Conference, December 2014,* pp. 436–445, https://doi.org/10.1145/2664243.2664257.

[23] Jeffrey Dalto, "The Three Phases of Risk Assessment: Risk Management Basics," Vector solutions, Convergence training, June 20, 2019, https://www.convergencetraining.com/blog/three-phases-risk-assessment-risk-management-basics.

[24] Jacqueline von Ogden, "3 Ways to Mitigate the Human Factors of Cyber Security," *CIMCOR*, June 20, 2017, https://www.cimcor.com/blog/3-ways-to-mitigate-the-human-factors-of-cyber-security.

[25] Brian M. Bowen, Ramaswamy Devarajan, and Salvatore Stolfo, "Measuring the Human Factor of Cyber Security," *IEEE Homeland Security Technology Conference,* November 15-17, 2011, https://doi.org/10.1109/THS.2011.6107876.

About the Authors

Flotilla Adm. Prof. Boyan **Mednikarov**, D.Sc. graduated first in class in the Naval Academy in Varna in 1984 and started his service at the missile ships brigade, as a Missile Officer. Subsequently, he went through the positions of Executive Officer, Commanding officer, Commander of a tactical group of ships, Chief of staff of squadron. The Admiral Kuznetsov Naval Academy in St. Petersburg, Russia awarded him a gold medal, when he obtained his second Master's degree in 1992.

During his extensive professional career, he has held the positions of a Senior Assistant Chief of the Operations Division at the Navy Headquarters in Varna, Deputy Head of the Operational-Tactical Department of the Postgraduate Centre at the Naval Academy, Head of the Naval Forces Department at the National Defence and Staff College. Between 2001 and 2011, he was the Deputy Rector of the Naval Academy in Varna. Since May 2011, he is the Rector of the Academy.

In 1999, he completed his PhD degree and later became an Associate Professor of Armed Forces Organization and Management. Flotilla Adm. Prof. Mednikarov has his third Master degree in Strategic Leadership of Defence and Armed

Forces from the National Defence and Staff College in Sofia. He has a Doctor of Science degree in Military-Political Aspects of Security. Since 2009, Flotilla Adm. Prof. Mednikarov is a Professor in the same academic field.

Prof. Mednikarov was the chairman of the Scientists' Union in Varna. He is a winner of the Varna Award for Science in 2008 in the field of social sciences. He was awarded the 2014 Prize of the Bulgarian Marine Chamber St. Nicholas for personal contribution in the development of marine science and education. Honorary Professor of the Naval Academy Mircea cel Batran, Constanta, Romania. Awarded with the Honorable Golden Order "Merit to Varna" in 2016 for the overall contribution to the development of marine education and science. Winner of the 2016 Black Sea Medal Awards for the long years of work in the field of conservation and improvement of the Black Sea environment. He was awarded a Doctor Honoris Causa Degree by Todor Kableshkov University of Transport, Sofia. Areas of expertise: Defence and Strategic Studies, Maritime Security and Safety, Maritime Education System, Leadership and Management in Shipping.

Colonel, Assoc. Prof. Yuliyan **Tsonev**, PhD, graduated the Artillery and Air-Defence Academy in 1986, "Military Cybernetics" speciality with honour. After his graduation he is involved in a team for developing automated IT and C4I systems. From 1989 to 1993 he is an assistant in the department of Computer Science in Artillery and Air-Defence Academy. He is a PhD student in Military Scientific Research Institute, Sofia and he got his PhD degree in 1994. In 2002 he is associate professor in Nikola Vaptsarov Naval Academy, where from 2014 onward he is the head of IT department. He is certified Cisco Academy Instructor (CCAI 887122) ; ITE, CCNA, CCNP, CCNA Security, Cyber Ops instructor. A wide experience as an administrator of Linux (Debian, RedHat), AIX, Windows servers (WEB, FTP, TFTP, DNS, Squid, MySQL); Cisco IOS operating system, configuration of Cisco IDS/IPS, ZBFirewall, ASA devices.

Prof. Andon **Lazarov** D. Sc. received the M.S. degree from Sent Petersburg Electro-Technical State University (LETI), Russia, in Electronic Engineering, a Candidate of Science (Ph.D.) degree from Minsk Air-Defence Military Academy, Belarus, and Doctor of Science degree from Shumen Artillery and Air Defence Academy. From 2000 to 2002 he is a Professor at the Air Defence Department of the Artillery and Air-Defence Academy. From 2002 to 2019 he is a Professor at Burgas Free University. Since 2019 he is a Professor at Nikola Vaptsarov Naval Academy – Varna. He teaches Discrete Mathematics, Coding theory, Antennas and Propagation, Communication circuits, Digital Signal Processing, Mobil Communications, Computer networks. His field of interests includes SAR-ISAR modelling and signal processing techniques. He has authored above 100 research journal and conference papers. He is a member of the IEEE, AES Society of USA, and of Trans Black Sea Region Union of Applied Electromagnetism in Greece. He is a member of the editorial and reviewer boards of many international journals in the USA, Canada, GB, China, Greece, etc.