THE ANNALS OF "DUNAREA DE JOS" UNIVERSITY OF GALATI
FASCICLE XI – SHIPBUILDING. ISSN (print) 1221-4620, ISSN (online) 2668-3156
2019

UNDERSTANDING OF THE CYBER RISK ONBOARD SHIP AND SHIP STABILITY

Remus Zăgan
Constanta Maritime University,
Maritime Cyber Security Centre of Excellence
Department, Constanta, Mircea cel Bătrân Street,
No. 104, Postal Code 900663, Romania,
E-mail: zagan.remus@cmu-edu.eu

Gabriel Raicu
Constanta Maritime University,
Maritime Cyber Security Centre of Excellence
Department, Constanta, Mircea cel Bătrân Street,
No. 104, Postal Code 900663, Romania,
E-mail: gabriel.raicu@cmu-edu.eu

ABSTRACT

In the last years cyber security has become a relevant issue for the maritime industry. The increasing digitalization in the maritime sector enables the remote communication between the ships and the headquarter company by means of information technology systems, and most of the operational technology (OT) equipment on board ships exchanges online communications data with the shore for monitoring the main functions of the ship. Failure the vessel operational technology (OT) equipment on board ship, like the ECDIS map for navigation, the steering systems and the main engine controls, has serious consequences. In this article we discussed the vulnerability of different OT equipments on board ship, and we highlighted how the hacker can inject some malware that affects the hull stress monitoring systems (HSMS), or can easy manipulate the EDI messaging text of the load plan (there is still a significant lack of security in the validation of message integrity) that finally leads to detrimental effects on the the ship's stability.

Keywords:. maritime, cybersecurity, ship planning system, hull stress monitoring systems, ship stability

1. INTRODUCTION

In these days, the maritime domain becomes a critical component of transportation and international trade. Statistics show that more than 90% of world's goods are travelling through sea lanes, which makes it crucial for the maritime community to understand the risks associated with the maritime cyber domain. The goods carried by sea, both in bulk and packaged, spend long periods of time in travel (the time spent during these voyages may be from 3 to 10 months), and there are various ships with both old and new systems. The ships cover in their voyages both zones with a very good connectivity or isolated ones, even if they have a narrow bandwidth for data communications.

It is known that the manoeuvrability and the stability of a vessel in waves are among the most important topics to be considered in ship design. Ship stability is a topic combining scientific rigor with experimental testing in basin. Ship stability, together with floatability and strength, are the most fundamental safety requirements in ship design.

The calculation of all forces acting on a vessel continues to be a challenging but important aspect of ship hydrodynamics, because of the large effect of these forces on rolling, and the consequent possibility of capsizing and loss of the ship.

The complexity and diversity of vessels' classes results in ships often having different operational computer systems installed on them.

According to the survey made in 2018 [9] the majority of software updates and patches (41%) were received on board by satellite. 26% arrived on board by DVD or on a memory stick and 29% by both satellite and DVD/memory stick. Only 4% were installed by shore-based IT staff or suppliers.

It is not to be overlooked that the vast majority of operating systems on ships dates back to over 30 years ago, so ships may have outdated systems, without technical support for software and hardware, which are prone to cyberattacks.

The new generations of modern ships have many devices with sophisticated equipment. The potential for sensitive technologies include the following (see Figure 1):

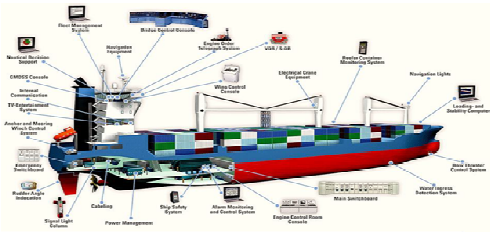

Fig.1. Electronic component on ship under cyber risk

Figure 1 focuses on equipments which permit to control the ship. A few of the ship's components look like this:

- Core infrastructure systems (Cabling, Security gateways, Routers, Wi-Fi system, Firewalls, VPN, etc.);
- Communication Systems, ECDIS, AIS, Radar/ARPA;
- Steering, VDR , GMDSS, eLORAN, VTS;
- Main engine with propulsion system;
- Cargo management systems;

Nowadays vessels are increasingly using systems that rely on automation, digitization, digitalization, which call for cyber risk management on board. In the future, information technology and operational technology continues to develop onboard ships, which are (or will be) frequently connected to the internet. All these increase the risk of unauthorized access or malicious attacks to vessels' equipments and networks. [2].

Cyber security together with cyber safety is very important because of their potential effect on the ship, company and cargo. Cyber security is concerned with the protection of IT, OT, information and data from unauthorized access, manipulation and disruption. Cyber safety covers the risks from the loss of availability or integrity of safety critical data and OT.

Fig.2. Cyber risk management approach as set out in the BIMCO guidelines, 3rd edition [2]

The expert in cyber security gives recommendation in the last guidelines launched in November 2019, which point to the necessity of implementating and maintaining of a cyber security management program in accordance with the approach in figure 2.

The vessels' management needs to stay engaged throughout the process, to ensure that the protection, contingency and response planning are balanced in relation to the threats, vulnerabilities, risk exposure and consequences of a potential cyber incident.

2. OT SYSTEMS & IT SYSTEMS

According to Gartner, OT means "the hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and

events in the enterprise", and IT is "the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services and does not include embedded technologies that do not generate data for enterprise use" [10].

Table 1 Typical differences between IT and OT systems [2]

Category	IT system	OT system
Performance requirements	• non-real-time • response must be consistent • less critical emergency interaction • tightly restricted access control can be implemented to the degree necessary for security	• real-time • response is time-critical • response to human and any other emergency interaction is critical • access to OT should be strictly controlled, but should not hamper or interfere with human-machine interaction
Availability (reliability) requirements	○ responses such as rebooting are acceptable ○ availability deficiencies may be tolerated, depending on the system's operational requirements	○ responses such as rebooting may not be acceptable because of operational requirements ○ availability requirements may necessitate back-up systems
Risk management requirements	▪ manage data ▪ data confidentiality and integrity is paramount ▪ fault tolerance may be less important. ▪ risk impacts may cause delay of: ship's clearance, commencement of loading/ unloading, and commercial and business operations	▪ control physical world ▪ safety is paramount, followed by protection of the process ▪ fault tolerance is essential, even momentary downtime may not be acceptable ▪ risk impacts are regulatory non- compliance, as well as harm to the personnel onboard, the environment, equipment and/or cargo
System operation	✓ systems are designed for use with commonly known operating systems ✓ upgrades are straightforward with the availability of automated deployment tools	✓ differing and possibly proprietary operating systems, often without built in security capabilities ✓ software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and possible involvement of modified hardware and software

Resource constraints	systems are specified with enough resources to support the addition of third-party applications such as security solutions	systems are designed to support the intended operational process and may not have enough memory and computing resources to support the addition of security capabilities

Operational technology (OT) systems differ from traditional information technology (IT) systems. OT is hardware and software that directly monitors/controls physical devices and processes. IT covers the spectrum of technologies for information processing, including software, hardware and communication technologies. Traditionally OT and IT have been separated, but with the internet, OT and IT are coming closer as historically stand-alone systems are becoming integrated. Disruption of the operation of OT systems may impose significant risk to the safety of onboard personnel, cargo, damage to the marine environment, and impede the ship's operation.

Based on [27], we present in the table 1, typical differences between IT and OT systems. There may be important differences between who handles the purchase and management of the OT systems versus IT systems on a ship.

Usually IT departments are not involved in the purchase of OT systems. The acquisition of such systems should involve the mechanical engineer, who knows about the impact on the onboard systems but will most probably only have limited knowledge of software and cyber risk management.

In accordance with the ISPS Code, the ship is obliged to conduct a security assessment, which includes identification and evaluation of key shipboard operations and the associated potential threats. Therefore, the ship's security plan may need to include appropriate measures for protecting both the equipment and the connection.

Table 2 Differences between IT and OT [12]

Attribute	**IT**	**OT**
Privacy	High	Low
Message integrity	**Low-Medium**	**Very High**
System Availability	Low-Medium	High
Authenticate	**Medium-High**	**High**
Proof of the integrity	High	Low-Medium
Time Critically	**Days Tolerated**	**Critical**
System Downtime	Tolerated	Not Acceptable
Interoperability	**Not Critical**	**Critical**
Computing resources	Unlimited	Very limited with older processor
Software changes	**Frequent**	**Rare**
Worst case impacts	Frequent Loss Data	Equipment Destruction

Due to the fast adoption of sophisticated and digitalized onboard OT systems, consideration should be given to including these procedures by reference to the SMS in order to help ensure the ship's security procedures are as up-to-date as possible.

Lack of physical and/or cyber security at a supplier within their products or infrastructure may result in a breach of corporate IT systems or corruption of the ship OT/IT systems.

3. IDENTIFY THREATS AND VULNERABILITIES AGAINST CYBER SECURITY POINT OF VIEW

Usually the experts in cybercrime try to identify what are the motivations for attackers, because these are necessary to establish the cyber security threat levels.

In the last years, attackers made a widespread influx of Ransomware all over the world, especially with a vew of having access at data companies.

In the maritime industry there are various suppliers involved in the international shipping operations, and for these reasons they are potential threats in the maritime supply chain and also pose a potential vulnerability in the chain [20].

Mapping the threats landscape we can identify the vulnerabilities arising from IT and OT systems.

The vulnerabilities of a system can relate to seven domains, as specified in the guidelines for the Protection of Industrial Systems on a ship published by the Maritime Affairs Directorate [17].

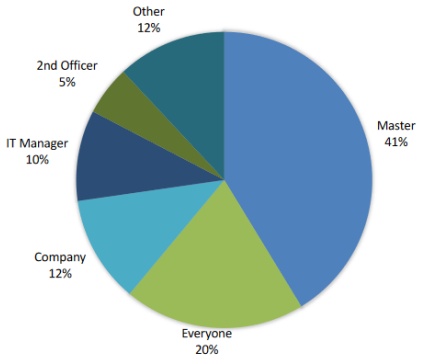

Fig.3. Responsible for ship cybersecurity [9]

In the shipping industry there are different types of threats that can be targeted at a specific maritime company, commercial ship or fleet.

Having in mind the vulnerabilities of maritime industry regarding cyber-attack, most of the crew members need to be training in cyber security. This conclusion result from the survey made in 2016 [9].

During the last 3 years, one of the main objectives of the International Maritime Organization (IMO) is marine safety and the protection of cyber security for the shipping industry.

IMO amended two of their general security management codes to explicitly include cyber security [11].

The European Union, through the Directive (EU) 2016/1148, has outlined the measures for a high common level of security of network and information systems across the Union from May 2016. The instructions include EU ports but not vessels [8].

Experts in cyber security from different maritime-concerned parties of the private and public sectors published different articles regarding maritime cyber security, such as the European Network and Information Security Agency (ENISA) [26], the International Maritime Organization (IMO) [11], the guidelines published by BIMCO [2], while the Det Norske Veritas (Norway) and Germanischer Lloyd (Germany), under acronym DNV-GL, published very good recommended practice as well [29].

The principal risk against cyber security is represented by the increased connectivity between OT onboard ships by digitalization.

Fig.4. Cyber attacks in shipping industry [23]

In the Figure 4 we illustrate the different types of threats in the shipping industry, resulting from the survey made by Baltic and International Maritime Council (BIMCO) [19].

From Figure 4 it results that the respondents mentioned that 77% represented attacks by malware and 57% by phishing.

It is important to achieve the integration of the digital communication of ships with head-

quarters in order to monitor the ships' parameters like engine performance, management for cargo, loading and unloading and stow planning also. These systems provide data which can be exploited by cyber criminals.

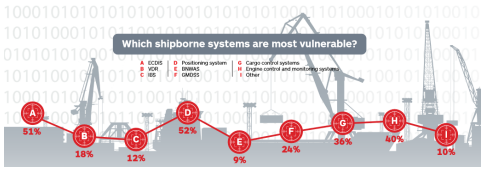

Fig.5. Vulnerability of the OT systems regarding cyber-attacks [23]

Some IT and OT systems are remotely accessible and may operate with a continuous internet connection for remote monitoring, data collection, maintenance functions, safety and security. These systems can be "third-party systems", whereby the contractor monitors and maintains the systems from a remote access. These systems could include both two-way data flow and upload-only.

Systems and work stations with remote control, access or configuration functions could, for example, be:

- ✓ stability decision support systems;
- ✓ cargo handling and stowage, engine, and cargo management and load planning systems;
- ✓ hull stress monitoring systems;
- ✓ bridge and engine room computers and work stations on the ship's administrative network;
- ✓ navigational systems.

4. MARITIME CYBER THREAT SCENARIOS

4.1. Hacking the HSMS

In this section we present several cyber attack scenarios based on known OT vulnerabilities.

Following the discussions with experienced commanders and mechanical officers regarding some vulnerability of the existing OT systems in the ship and extrapolating the consequences of cyber-attacks resulted in the scenarios that we present below.

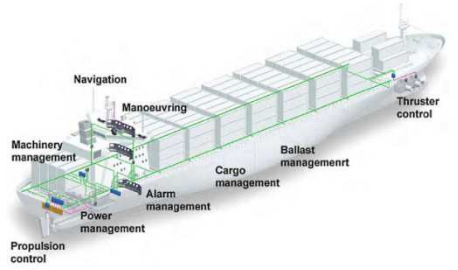

Fig.6. Principal OT systems interconnected on a ship [33]

In the figure 7 we present part of connection between OT systems on ship.

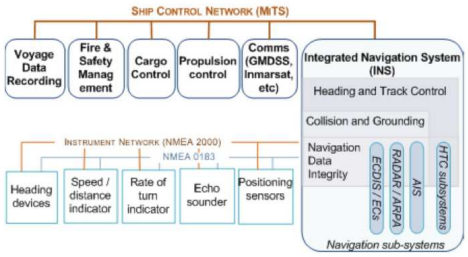

Fig.7. Connection between OT systems on ship [18]

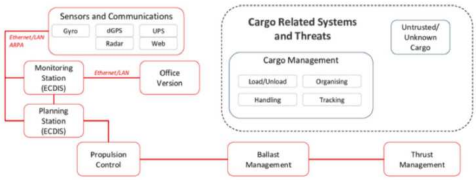

Fig.8. Connections between OT systems like navigation with propulsion and cargo [16]

A possible interdependence between Ballast Management and Thrust Management results from the figure 8.

Similar to classical Open Systems Interconnection model (OSI) [3], in figure 9 we present the NMEA 2000 which consists in few communication layers.

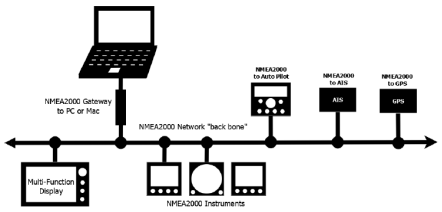

Fig.9. Typical NMEA 2000 diagrams [32]

The hardware and software used for satellite communication were analyzed by the pen-tester expert Ken Munro [31], who found that the administration interface was done over unencrypted HTTP and unencrypted telnet protocols.

Electronic Crane Equipment and Main Ballast System compose the Cargo management, systems that usually are automatized on ships. Onboard loading computer and other computers used for an exchange of loading information, provide stability control and load plan updates with the marine terminal and stevedoring company.

NMEA networks are used to communicate between OT systems on ship and it was proven that there is no encryption, authentication, integrity on this communications.

The system that is responsible for measuring various forces acting on the hull is representing by Hull Stress Monitoring System (HSMS) that uses electronic strain gauges and accelerometers to feed data to on board monitoring systems.

The cargo ships are designed with certain limits of the load for each force type, and every excess strain is detected when we have the loading operations, alarming the crew to take action when the limit values are exceeded. Inadequate loading of the warehouses of the ship can lead to sagging or hogging phenomena (see figure 12).

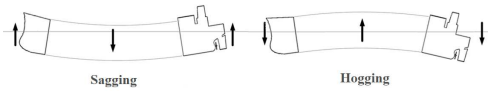

Fig.10. The possible forces which bends the hull

In general, the ship's crew, during ship loading operations, rely on automatic stress monitoring systems, and thus there is a likelihood that a hacker will be able to manipulate loading data that is fed to and from the loading monitoring system. The hacker has two alternatives, first by compromising the communication network through a phishing attack, and the second by directly attacking the existing satcom unit on the ship. The system being altered the operation of loading the ship will continue, without the occurrence of alert alarms regarding exceeding values.

It is possible for the hacker to display on the monitor forces that correctly indicate the ship's loading, but in reality the forces will be altered in value.

Based on the discussions with those operating the commercial vessels, a number of risks have been identified to exist within the OT systems of the ship, namely:

•the existence of Windows XP / 98/95 operating systems, which represent versions without technical support of antivirus protection;

•communication between OT systems is done without data encryption;

•the access to the data transmitted between the ship and the headquarter is achieved without a minimum of protection of checking the authorization of the transmitter//receiver the respective data.

4.2. Hacking the Container Load Plan or altering the EDIFACT message

The crew of the ship are using the USB pen drives or a floppy disks, for giving information regarding the Container Load Plan, when handling the containers from the dock to the ship.

In order to be able to alter the ship's planning system or modify the loading plan, we must understand the complexity of the EDIFACT messaging system that is used to create ship loading and container storage plans.

The EDIFACT messaging system consists of the many electronic messages exchanged between the transport lines, port authorities,

terminals and ships. The EDIFAC messaging system has many versions, and between them there are significant differences.

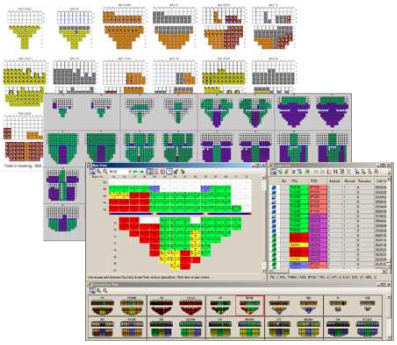

Fig.11. Container arrangement inside the ship

In general, hackers are less interested in destabilizing ships, but, for them, it is of interest to redirect containers for theft of goods.

A sample EDIFACT message might look like this:

```
UNB+UNOC:3+SENDER ID:ZZZ:                    UNB   Interchange header
SENDER INT ID+RECEIVER ID:ZZZ:
RECEIVER INT ID+201511128:1037+1++++1++1'
UNH+1+ORDERS:D:01B:UN'                       UNH   Message header
BGM+220+PO357893+9'                          BGM   Beginning of message
                                                   Section for Buyer is always first
DTM+2:200808131430:102'                      DTM   Delivery date
DTM+2:20151128:203'                          DTM   Document date
FTX+DEL+1++INCLUDE TIME IN DELIVERY DATE'    FTX   Free text
RFF+AAN:APPTNO123445'                        RFF   Reference
NAD+AA+Buyer_Id_12345::1'                    NAD   Name and address
LOC+1+Buyer Place Warehouse 678::1'          LOC   Location identifier
CTA+PD+BuyerEmployee1234:John Smith'         CTA   Contact information
COM+Buyer_email@BuyerCompABC.com:EM'         COM   Communication contact
                                                   Section for Ship To next
NAD+AA+ShipTo_Id_87654::1'                   NAD   Name and address
LOC+1+ShipTo_Id_87654::1'                    LOC   Location identifier
CTA+PD+BuyerEmployee1234:John Smith'         CTA   Contact information
COM+ShipTo_Id_87654:EM'                      COM   Communication contact
                                                   Section for shipping line info
LIN+1+1+1'                                   LIN   Line item
PIA+5+ENT-93474:BH'                          PIA   Additional product ID
IMD+F++:::Product Description'               IMD   Item description
MEA+AAA++EA:1'                               MEA   Measurements
QTY+21:3:A1B'                                QTU   Quantity
PRI+INV:3455.58'                             PRI   Price details
                                                   Section control
UNS+S'                                       UNS   Section idenfication
MOA+1:4406.57'                               MOA   Monetary amount
CNT+2:2'                                     CNT   Control total
UNT+30+1'                                    UNT   Message trailer
UNZ+1+1'                                     UNZ   Interchange trailer
```

Fig.12. Sample EDIFACT message [36]

To change EDIFACT one needs only to manipulate the segment values inside the message.

An example consists in manipulating container weight and ship balance, and we can alterate the text in this way:

MEA+AAE+VGM+KGM:1550.7′ or MEA+AAE+VGM+LBR:5550'

VGM is the Verified Gross Mass, KGM is kilos and LBR is pounds.

By altering the values from kilograms to pounds, the ship may be heavier or lighter, and the ship loading planning software will determine the location of the container in an inappropriate area, thus affecting the stability of the ship.

Another example consists in changing the attributes for a container that needs special handling, maybe by indicating that it is explosive:

ATT+26+AGR:DGATT:306+XS:DGAGR:306′ - describes the existence of explosive materials.

We can change the message : ATT+26+AGR:DGATT:306+S:DGAGR:306′

Fig.13. Hull failure incident on the MOL Comfort [34]

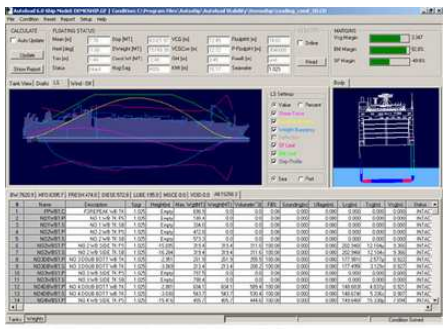

Fig.14. Computing longitudinal strength and ship stability [35]

A potential cause of the MOL Comfort breaking in two in the middle area of the ship could be improper loading of containers, or the

existence of a crack or structure defect in the hull area, or the validity of both hypotheses.

It is possible that the loading programs now allow the mates to compute longitudinal strength.

5. CONCLUSIONS

Most cyber-attacks that take place in the shipping industry remain confidential. Cyber security experts have a duty to shed light on possible cyber-attack scenarios on the maritime industry and to expose the vulnerabilities of OT systems to such attacks. The virtual scenarios of cyber-attacks on the ship's systems highlight the financial damage they cause to shipping, maritime and port infrastructure, as well as the risk of loss of life.

In this paper we presented the risks of a cyber-attack given by the manipulation of the HMSC system as well as the alteration of the EDIFACT messages.

At the same time, there is the possibility of altering the EDIFACT messages regarding the billing, which gives the hacker the opportunity of a financial fraud by changing the message regarding the bank account number for the delivery of the money.

In conclusion, the integrity of the messages EDIFACT OR BAPLIE is essential in order to avoid financial losses as well as the safety of container transport.

The main objectives of the shipping industry regarding the cyber-attack are to ensure that no malicious act can endanger the operation of the ship.

"80 percent of the cybersecurity incidents could have been prevented if single users were able to recognize the threat. It is vitally important to educate the crew on board in order to raise awareness about the vulnerabilities arising from human error."

REFERENCES

[1]. **American Bureau of Shipping**, *"The application of cybersecurity principles to marine and offshore operations",* volume 1: Cybersecurity, February 2016.

[2]. **BIMCO,** *"Guide version 3 November" 2019,* https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20

[3]. **Blog of Lasse Karstensen**, *"Varnish, Sailing and occasional weekend hacks", (August 2016). NMEA2000 and CANbus, online -* https://lassekarstensen.wordpress.com/2016/08/09/nmea2000-and-canbus/

[4]. **Chițu M.G., Manea E., Bormambet M.**, *"Modelation of the oscillatory motions of the ship for the Mediterranean sea navigation conditions, using the OCTOPUS software",* Analele Universităţii Maritime din Constanţa, an XIV, Vol.19, 2013, pag 37-44, 2013*;*

[5]. **Chițu M.G., Zăgan R., Manea E**, *"Dependence analysis for the amplitude oscillatory movements of the ship in response to the incidence wave",* ModTech International Conference, Modern Technologies in Industrial Engineering, 17-20 iunie 2015*,* https://iopscience.iop.org/1757-899X/5/1 *;*

[6]. **Chițu G., Zăgan R.**,*"Comparative study of dynamic nautical features of turning computer asist and sea trial",* International Journal of Modern Manufacturing Technologies ISSN 2067–3604, Vol. I, No. 1, page 21-24, 2009;

[7]. **Chițu G.M., Zăgan R.**, *"Prediction for roll and roll cross-vertical oscillatory motions of the ship in the real sea using OCTOPUS", International* Conference MODTECH 2013: Modern Technologies in Industrial Engineering, Sinaia, 27-29 June, ISSN 2067–3604, pp. 40-49, Vol. VI, No. 1, 2014;

[8]. **European Parliament. Directive** *(EU) 2016/1148. "Official Journal of the European Union",* 2014(L194):1–30, 2016;

[9]. **Futurenautics Research**. *"Crew Connectivity 2018 Survey Report"*. page 29, 2018;

[10]. **Gartner**. *"It glossary, online"*. https://www.gartner.com/it-glossary, 2018;

[11]. **IMO**, *"Interim guidelines on maritime cyber risk management",* IMO-MSC 1/CIRC 1526 June 1st edited in June 2016.

[12]. **Information Security Audit and Control Association,** *"The Merging of Cybersecurity and Operational Technology",* pages 1–8, 2016;

[13]. **INTERIM GUIDELINES ON MARITIME CYBER RISK**

MANAGEMENT, *MSC.1/Circ. 1526,* 1 June 2016;

[14]. **Kimberly Tam, Kevin Jones**, *"Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping",* Journal of Cyber Policy on August 29th 2018, available online: https://www.tandfonline.com/doi/full/10.1080/23738871.2018.1513053

[15]. **Lloyd's Register's**, *"Cyber-enabled ships, Deploying information and communications technology in shipping",* First edition, February 2016;

[16]. **Maria Papadaki, Kimberly Tam, Kevin D. Jones**, *"Threats and Impacts in Maritime Cyber Security",* https://www.researchgate.net/publication/304263412_Threats_and_Impacts_in_Maritime_Cyber_Security

[17]. **Richard Benham and James Sproule**, *"Cyber Security",* IOD Policy Report March, 177, 2017;

[18]. **Skema** , *"Interactive Knowledge Platform For Transport And Logistics, Navigation systems including developments in e-navigation",* 2019, http://www.eskema.eu/defaultinfo.aspx?topicid=47&index=4

[19]. **BIMCO,** *"Story in numbers with BIMCO", online* - https://cybersail.org/wp-content/uploads/2017/02/IHS-BIMCO-Survey-Findings.pdf *, 2016;*

[20]. **Sotiria Lagouvardou**, *"Maritime Cyber Security:concepts, problems and models",* Master Thesis 2018;

[21]. **Zăgan R., Raicu G., Hanzu-Pazara R., Enache S.,** *"Realities in maritime domain regarding cyber security concept",* Proceedings of ADEM Conference 2016, Drobeta Turnu Severin, publishing in the Trans Tech Publication volume (book) Advances in Engineering and Management ISSN 1662–8985, Issue 881, page 221-228, DOI: 10.4028/www.scientific.net/AEF.27.221, 2016;

[22]. **Zăgan R., Chiţu G.M., Manea E.**, *"Ship manoeuvrability prediction using wavelets and neural networks",* International Conference MODTECH 2014: Modern Technologies in Industrial Engineering, Gliwice, 13-16 July, 2014, Proceedings of MODTECH 2014 International Conference, Advanced Materials Research ISSN 1662–8985, Issue 1033-1036, p946-951, 2014;

[23]. https://cybersail.org/wp-content/uploads/2017/02/IHS-BIMCO-Survey-Findings.pdf

[24]. **CyberKeel**, *"Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas",* Copenhagen: CyberKeel, http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf , 2014;

[25]. http://www.safety4sea.com/wp-content/uploads/2016/02/ESC-White-paper-on-Maritime-Cyber-Security-2016_02.pdf

[26]. **ENISA**, *"Cyber Security Aspects in the Maritime Sector"* https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1 ,

[27]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[28]. https://navarino.gr/wp-content/uploads/2018/04/Crew_Connectivity_2018_Survey_Report.pdf

[29]. **DNV-GL- RP-0496**, *"Cyber security resilience management for ships and mobile offshore units in operation",* http://www.gard.no/Content/21865536/DNVGL-RP-0496.pdf , edition September 2016;

[30]. http://www.engineersjournal.ie/2014/07/17/merchant-shipping-and-the-marine-engineering-technology-revolution/

[31]. https://www.pentestpartners.com/security-blog/hacking-tracking-stealing-and-sinking-ships

[32]. http://signalk.org/overview.html

[33]. http://www.shippipedia.com/ship-automation-control-system/

[34]. http://archive.indianexpress.com/news/merchant-vessel-mol-comfort-splits-into-two-off-mumbai-coast-crew-rescued/1130174

[35]. http://www.coastdesign.no/products/loading-computer/?article_id=64

[36]. https://www.pentestpartners.com/security-blog/making-prawn-espressos-or-hacking-ships-by-deciphering-baplie-edifact-messaging/

University of Galati, Fascicle XI Shipbuilding, pp.19-24, 2016.

Paper received on November 09th, 2019